



Identiteettivarkaus ja sen vaikutukset uhriin

Puro, Jessica

2017 Hyvinkää



Laurea-ammattikorkeakoulu
Hyvinkää

Identiteettivarkaus ja sen vaikutukset uhriin

Puro, Jessica
Liiketalous
Opinnäytetyö
Elokuu, 2017

Puro, Jessica

Identiteettivarkaus ja sen vaikutukset uhriin

Vuosi	2017	Sivumäärä	40
-------	------	-----------	----

Tämän opinnäytetyön tavoitteena oli selvittää identiteettivarkauden kriminalisoinnin määritelmiä ja siihen liittyvää sääntelyä sekä tutkia, mitä vaikutuksia rikoksella on uhriin ja kuinka uhrin on mahdollista ennaltaehkäistä tai suojautua identiteettivarkausrikoksilta. Tarkoituksena oli selvittää, millainen on tyypillinen identiteettivarkauden uhri, miten rikos vaikuttaa uhriin psyykkisesti, sosiaalisesti ja taloudellisesti sekä millä tavoin uhrin on mahdollista ennaltaehkäistä identiteettivarkauden uhriksi joutumista tai suojautua identiteettivarkauden vaikutuksilta.

Tietoperustan lähteinä käytettiin pääasiassa oikeuskirjallisuutta, hallituksen esityksiä, EU:n direktiivejä ja asetuksia, lehtiartikkeleita, voimassa olevaa lainsäädäntöä sekä vertailuna osittain aiempaa lainsäädäntöä. Lisäksi lähteinä käytettiin erilaisia lausuntoja sekä työryhmi-en loppuraportteja. Opinnäytetyötä lähestyttiin oikeusdogmaattisesta näkökulmasta, mutta kriminalisointia ja aiempaa lainsäädäntöä verrattaessa lähestyttiin opinnäytetyötä myös vertailuvan tutkimuksen kautta. Uhrin asemaa ja vaikutuksia tarkasteltaessa käytettiin osaltaan myös arvoperusteista tulkintaa.

Tutkimuksen alussa tarkasteltiin identiteettiä, ja opinnäytetyötä lähestyttiin 2015 voimaan astunutta identiteettivarkauksien kriminalisointia rikoslaissa tarkastelemalla. Identiteettivarkauksia tarkasteltiin paitsi traditionaalisesta näkökulmasta, myös tietoverkossa tapahtuvien rikosten kautta. Teknologian jatkuvan kasvun ja kehityksen myötä ovat esimerkiksi sosiaalisissa medioissa tapahtuvat identiteettivarkaudet yleistyneet huomattavasti, ja se on myös osaltaan mahdollistanut ja helpottanut kyseisten rikosten tekoa. Rikosten määrällisen lisääntymisen ja rikossenteon helpottumisen myötä on tärkeää, että uhri tietää, kuinka voi suojautua vastaavanlaisilta rikoksilta tai kuinka toimia, jos joutuu rikoksen kohteeksi siitä huolimatta.

Lopputuloksena on kuvaus identiteettivarkaudesta rikoksena sekä uhrin asemasta ja rikoksen vaikutuksista uhriin. Opinnäytetyössä on myös tuotu esiin erilaisia keinoja ennaltaehkäistä uhriksi joutumista sekä suojautua identiteettivarkauden vaikutuksilta niin sosiaalisesti kuin taloudellisesti. Lopputuloksissa on myös huomioitu identiteettivarkauksiin ja niiden kriminalisointiin liittyviä ongelmia sekä erilaisia kehitysehdotuksia näiden ongelmien poistamiseksi tai vähentämiseksi.

Asiasanat: Identiteettivarkaus, uhrin asema, rikoslaki, kriminalisointi, ennaltaehkäisy

Puro, Jessica

Identity theft and its impact on a victim

Year	2017	Pages	40
------	------	-------	----

The main goal of this thesis was to examine the definitions and regulations behind the criminalization of identity theft and to research its impact on the victim and how it is possible for the victim to prevent or protect themselves from identity theft crimes. The intent was to clarify what is the typical victim of an identity theft like, how the crime affects the victim physically, socially and financially and how it is possible for the victim to prevent becoming the victim of an identity theft or to protect themselves from the effects of an identity theft.

The thesis is based on legal literature, legislative proposals of the government, directives and decrees of the European Union, newspaper articles, current legislation and partly the previous legislation for comparison purposes. Bibliography also includes statements and final reports of working committees. The thesis was approached from a legal dogmatic viewpoint and considered a comparison of criminalization and previous legislation, also through a comparative research method. While examining the status and impacts on the victim, a value-based interpretation was also used.

The research began with the examination of identity, and the thesis was approached through inspection of the identity theft criminalization that came into effect in 2015. Identity thefts were examined not only from the traditional point of view, but also through network-based crimes. Along with the consistent growth and evolution of technology, the identity thefts taking place in social media for example have become more frequent and it has for its own part enabled and eased the acts of the said crimes. Because of the quantitative growth and the ease of committing such crimes, it is important for the victim to know how to protect themselves against identity theft and how to act if they are victimized regardless.

The result of the thesis is a description of identity theft as a crime and the status and impact of the crime on the victim. The thesis offers different ways for the victim to prevent themselves becoming a victim and to protect themselves from the social and financial impacts of identity theft. Conclusions also address complexities regarding identity theft and their criminalization, and offers proposals of improvement to remove or decrease these said problems.

Keywords: Identity theft, status of the victim, criminal law, criminalization, prevention

Lyhenneluettelo

EU	Euroopan unioni
EY	Euroopan yhteisö
HE	Hallituksen esitys
HeTiL	Henkilötietolaki (523/1999)
JulKL	Laki viranomaisten toiminnan julkisuudesta (621/1999)
LaVM	Lakivaliokunnan mietintö
OM	Oikeusministeriö
RL	Rikoslaki (39/1889)
SM	Sisäministeriö
TYK	Tietoyhteiskuntakaari (917/2014)
YksTL	Laki yksityisyyden suojasta työelämässä (759/2004)

Sisällys

1	Johdanto	7
2	Identiteettivarkaus	8
2.1	Identiteettivarkauden määritelmä ja kriminalisoinnin taustat	10
2.2	Identiteettivarkauden muodot	12
2.3	Teon tarkoitukset	13
2.4	Rangaistavuus ja mahdolliset rikosnimikkeet ennen kriminalisointia	15
3	Identiteettivarkauden uhri	18
3.1	Uhrin asema identiteettivarkauksissa	19
3.2	Vaikutukset uhriin	21
3.2.1	Sosiaaliset seuraukset	23
3.2.2	Taloudelliset seuraukset	25
3.2.3	Psyykkiset seuraukset	26
3.3	Ennaltaehkäisy ja suojautuminen	29
3.3.1	Verkkoidentiteettivarkauksien ennaltaehkäisy uhrin toimesta	32
3.3.2	Perinteisten identiteettivarkauksien ennaltaehkäisy uhrin toimesta ...	33
3.3.3	Rikoksen vaikutusten minimalisointi ja vaikutuksilta suojautuminen ...	34
4	Johtopäätökset	35
	Lähteet	38
	Taulukot	40

1 Johdanto

Jotta voidaan tarkastella identiteettivarkautta, on ensin ymmärrettävä itse identiteetin määritelmä. Käsitteenä se on äärimmäisen moniselitteinen, ja identiteetistä puhuttaessa voidaan tarkoittaa kulttuurista identiteettiä tai psykologista identiteettiä, niin sanottua minäkuva. Tavanomaisesti identiteetistä puhuttaessa tarkoitetaan sitä, kuka ihminen on ja mistä hänet tunnetaan ja tunnistetaan.¹ Arkisessa kontekstissa identiteetillä tarkoitetaan usein siis esimerkiksi luonnetta, persoonallisuutta tai henkilöllisyyttä, niin sanottua psykologista identiteettiä. Kulttuurinen identiteetti taas muodostuu erilaisista henkilön ominaisuuksista, kuten sukupuolesta tai ihonväristä, kansalaisuudesta tai kulttuurista. Identiteettiä ei tule kuitenkaan sekoittaa yhteiskunnan ja sen normien määrittämiin rooleihin, kuten vanhempi tai työntekijä, vaan se rakentuu henkilön yksilöllistymisprosessin mukana. Pohjimmiltaan identiteetti on se omien tarkoitusten ja kokemusten summa, joka erottaa henkilön muista.²

Identiteetti voidaan teoriassa myös jakaa kahteen eri osa-alueeseen. Ensimmäinen osa identiteetistä ja siihen kuuluvista ominaisuuksista saadaan heti syntyessä, kun taas toinen osa luodaan vasta myöhemmin. Myöhemmin rakentuva osa identiteettiä ovat aiemminkin mainitut piirteet kuten persoonallisuus tai luonne. Näitä syntymässä määräytyviä identiteetin osia taas ovat erilaiset biometriset tunnistetietot kuten sormenjäljet, ääni, kasvojen muodot ja DNA. Syntymässä määräytyviin identiteetin osiin ei itse voi vaikuttaa, kun taas myöhemmin rakentuvaan osaan identiteettiä vaikuttavat omat kokemukset ja kulttuuri sekä ympäristö.³

Tässä opinnäytetyössä identiteettiin viitattaessa tarkoitetaan niitä henkilön ominaisuuksia, joiden avulla hänet voidaan yksilöidä tai tunnistaa esimerkiksi viranomaisen toimesta. Persoonallisuus, luonne tai muut perinteisemmän näkökulman identiteetin piirteet eivät tässä yhteydessä ole olennaisia muutoin kuin sosiaalisia vaikutuksia tarkasteltaessa, sillä identiteettivarkauksia tarkasteltaessa merkitys painottuu lähinnä juridiseen identiteettiin eli henkilöllisyyteen ja yksilöllisiin tunnistetietoihin, syntymässä määrittyviin biometrisiin identiteetin osiin sekä henkilötietoihin. Henkilötietojen kuten nimen, sosiaaliturvatunnuksen tai luottotietojen haltuun saaminen ja väärinkäyttö voi johtaa identiteettivarkauteen, sillä henkilökohtaisia tunnistetietoja on mahdollista käyttää esiintyäkseen toisena henkilönä, jonka avulla on mahdollista tehdä useita erilaisia petoksia.

¹ Forss 2014, s. 83.

² Castells 2009, s. 6-7.

³ Forss 2014, s. 83

Identiteettivarkauksia tarkasteltaessa merkittävässä asemassa on syksyllä 2015 voimaan astunut identiteettivarkauksia koskeva rikoslain⁴ 38 luvun 9a §, joka säätelee kyseiset rikokset rangaistaviksi. Myös EU on osaltaan puuttunut kansallisen tason sääntelyyn asettamallaan tietoverkkorikosdirektiivillä⁵, jonka täytäntöönpanon kautta lainsäädäntöä alun perin lähdettiin muuttamaan. Identiteettivarkauksien tarkastelua ei voida kuitenkaan rajoittaa ainoastaan rikoslakiin ja sen uudistukseen, vaan on tarkasteltava myös erilaisia perusoikeuksia. Tärkeimmät identiteettiin ja siihen liittyviin rikoksiin linkittyvät osa-alueet ovat yksityisyyden suoja, henkilötietojen suoja ja itsemääräämisoikeus.

Tämä opinnäytetyö antaa kokonaiskuvan siitä, kuinka identiteettivarkaus määritellään ja mitä siitä on säädetty lainuudistuksen myötä. Opinnäytetyön tarkoitus on selvittää identiteettivarkauden vaikutuksia uhuriin sekä uhrin mahdollisuuksia suojautua rikoksilta ja ennaltaehkäistä rikoksen uhriksi joutumista. Opinnäytetyössä käydään läpi identiteettivarkauksiin liittyvää oikeuskäytäntöä sekä ennen että jälkeen kriminalisoinnin. Keskipisteenä on uhrin asema ja uhuriin kohdistuvat psyykkiset, sosiaaliset ja taloudelliset vaikutukset. Opinnäytetyössä lähteenä on käytetty pääasiassa oikeuskirjallisuutta, lainsäädäntöä, hallituksen esityksiä sekä erilaisia lehtiartikkeleita. Tutkimuksessa tarkastellaan aihetta nimenomaan uhrin näkökulmasta ja uhuriin kohdistuvien vaikutusten kautta, ei itse rikoksen tekijän tai teon motiivien kautta.

2 Identiteettivarkaus

Identiteettivarkausrikoksista puhuttaessa termi identiteettivarkaus on jokseenkin harhaanjohtava, sillä identiteetti itsessään ei ole irtainta omaisuutta vaan aineeton, henkilöä itseään kuvaava ominaisuus. Näin ollen identiteettiä sanan todellisessa merkityksessä ei voida varastaa, ainakaan rikoslain varkauden määritelmän⁶ tarkoittamalla tavalla. Suomen kielessä muita termejä ei ainakaan toistaiseksi ole kovinkaan aktiivisessa käytössä, mutta esimerkiksi englanninkielestä käännettäessä olisi mahdollista saada huomattavasti kuvaavampia termejä, kuten identiteettipetos (identity fraud) tai identiteetin kopioiminen (identity cloning). Kun puhutaan identiteettivarkauksista, puhutaan todellisuudessa tilanteesta, jossa kaksi ihmistä käyttää samaa identiteettiä.⁷

Sisäministeriön henkilöllisyyden luomista koskevan hankkeen työryhmä määritteli vuonna 2010 julkaisemassaan loppuraportissa⁸ identiteettivarkauden seuraavasti; Identiteettivarkaus on

⁴ RL 39/1889

⁵ Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU.

⁶ RL 28:1

⁷ Korhonen 2013, s. 287.

⁸ SM 32/2010

yleiskielessä käytetty käsite joukolle erilaisia tekokokonaisuuksia, joissa identiteettitietoa sekä kerätään että käytetään oikeudetta joko rikoshyödyn hankkimiseksi tai tavalla, josta aiheutuu identiteetin haltijalle vahinkoa tai muuten loukkaa uhrin oikeusturvaa. Identiteettivarkauden käsitteen tulisi kattaa myös teot, jotka loukkaavat henkilön itsemääräämisoikeutta aiheuttamatta selkeätä vahinkoa tai haittaa. Identiteettivarkaus on nimityksenä jossain määrin harhaanjohtava, sillä toisin kuin varkausrikoksessa, identiteettivarkaudessa identiteettiä ei välttämättä oteta pois rikosuhriin hallusta. Rikoksentekijä vain kopioi tiedon myös omaan käyttöönsä.⁹

Identiteettivarkauksia esiintyy erilaisissa muodoissa ja eri syistä, yleisimpänä näistä esiintyminen toisen henkilöllisyydellä, useimmiten petoksen suorittamiseksi. Rikoksen tekijä hankkii itselleen tietoa toisen henkilön perus- ja henkilötiedoista kuten asumistiedoista, pankkitiedoista tai sosiaaliturvatunnuksesta. Hankkimiaan tietoja tekijä käyttää tämän jälkeen omaksi hyödykseen, esimerkiksi ostamalla tai tilaamalla omaisuutta väärällä identiteetillä ja tämän johdosta toisen henkilön laskuun. Jo nämä perustiedot riittävät suuren taloudellisen vahingon tekoon, varsinkin nykyisin verkkokauppojen yleistyttyä. Varastetuilla henkilötiedoilla voidaan esimerkiksi ottaa pankkilainaa, avata puhelinliittymiä tai ottaa niin sanottuja pikavippejä.¹⁰ Identiteettivarkautta voidaan verrata esimerkiksi kotimurtoon siinä määrin, että tuntematon henkilö on päässyt uhrin yksityisimmälle alueelle ja penkonut kaiken, mitä on käsiinsä saanut. Lisäksi verkossa tapahtuvissa identiteettivarkauksissa uhri ei välttämättä koskaan saa tietää mitä tietoja identiteettivarkas on saanut käsiinsä tai missä ja milloin niitä jaetaan mahdollisesti eteenpäin.¹¹

Identiteettivarkaus on määritelty rangaistavaksi Suomen rikoslainsäädännössä vuoden 2015 lainuudistuksen¹² myötä, ja kriminalisoinnin seurauksena ilmoitusten määrä onkin ollut jatkuvassa nousussa. Helsingin sanomien artikkelissa¹³ keväältä 2017 on poliisin tilasto josta ilmenee ilmoitusten nouseva määrä, ja esimerkiksi Helsingissä on vuoden 2015 aikana tilaston mukaan ilmoitettu 188 identiteettivarkausrikosta, kun vuonna 2016 vastaava luku on ollut jo 948. Aamupostin artikkelin mukaan¹⁴ poliisille on tehty vuoden 2017 kevään aikana jo 1 643 ilmoitusta, kun esimerkiksi 2016 samaan aikaan ilmoituksia oli tehty 1 339. Koska identiteettivarkaudet yleistyvät ja ilmoitusten määrä nousee tasaisteen tahtiin, on erityisen tärkeää, että tapauksia voidaan ennaltaehkäistä ja tiedetään kuinka identiteettivarkaudelta on mahdollista suojautua.

⁹ SM 32/2010, s. 47.

¹⁰ Haasio 2013, 46-47.

¹¹ Tranberg & Heuer 2013, s. 96.

¹² HE 232/2014

¹³ Helsingin Sanomat 25.2.2017, digilehti. Viitattu 19.7.2017

¹⁴ Aamuposti 9.7.2017, s. 4. Viitattu 19.7.2017

2.1 Identiteettivarkauden määritelmä ja kriminalisoinnin taustat

Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.¹⁵ Näin Suomen rikoslaki määrittelee identiteettivarkauden. Ongelmallisena tässä voidaan nähdä etenkin se, ettei rikoksesta aiheudu minkäänlaista rangaistusta, ellei uhrille aiheudu vaikkapa taloudellista vahinkoa. Toisaalta taas voidaan identiteettivarkauden kriminalisointia itsessään pitää askeleena eteenpäin, mutta toisaalta taas on selvää, että tarve spesifioida identiteettivarkauden kriminalisointia tulee olemaan edessä ennemmin tai myöhemmin.

Tässä vaiheessa voidaankin kysyä, kuinka kriminalisointiin alkujaan päädyttiin, ja miksi juuri tällä määritelmällä. Lainuudistus alkoi Euroopan unionin syksyllä 2013 asettamasta tietoverk-korikosdirektiivistä¹⁶, joka edellytti jäsenvaltioita toteuttamaan tarvittavat toimenpiteet varmistaakseen, että direktiivin 3-8 artiklassa tarkoitetuista rikoksista voidaan määrätä tehokkaat, oikeasuhteiset ja varoittavat rikosoikeudelliset seuraamukset. Uudistuksen tuli olla saatettuna voimaan kansallisella tasolla 4. syyskuuta 2015 mennessä. Vaikka direktiivissä vaaditut uudistukset koskivatkin tietojärjestelmiin tunkeutumista, datan vahingoittamista, järjestelmän häirintää ja viestintäsalaisuuden loukkaamista, oli direktiivissä mainittu, että "Jäsenvaltioiden on toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että jos 4 ja 5 artiklassa tarkoitetut rikokset on tehty käyttämällä väärin toisen henkilön henkilötietoja tarkoituksena voittaa kolmannen osapuolen luottamus ja aiheuttaen näin vahinkoa henkilöllisyyden oikealle omistajalle, tätä voidaan kansallisen lain mukaisesti pitää raskauttavana asianhaarana, jolleivät nämä asianhaarat jo kuulu jonkin muun kansallisen lain mukaisesti rangaistavan rikoksen tunnusmerkistöön"¹⁷. Kyseinen identiteettivarkauteen viittaava kohta saikin aikaan myös identiteettivarkauden tarkastelua yksittäisesti kansallisella lainsäädäntötasolla sekä esittämään lakimuutosta myös sitä koskevilta osin.

Kun hallituksen esitys direktiivin täytäntöönpanoksi tehtävistä lakimuutoksista annettiin, oli sinne lisätty myös identiteettivarkaus. Hallitus esitti rikoslain 38 lukuun lisättäväksi direktiivin velvoitteiden täytäntöönpanoksi identiteettivarkautta koskevaa pykälää. Syyteoikeutta koskevan 10 §:n mukaan identiteettivarkaus olisi asianomistajarikos, ja se lisättäisiin myös sotilas-

¹⁵ RL 38:9a

¹⁶ 2013/40/EU

¹⁷ 2013/40/EU 9 artiklan 5 kohta.

oikeudenkäyntilain 2 §:ssä tarkoitettujen sotilasoikeudenkäyntiasiana käsiteltäviin rikoksiin.¹⁸ 27. syyskuuta 2013 oikeusministeriö asetti työryhmän valmistelemaan lakiehdotusta, ja työryhmässä oli oikeusministeriön ohella edustajia sisäministeriöstä, liikenne- ja viestintäministeriöstä, valtakunnansyyttäjänvirastosta, tietosuojavaltuutetun toimistosta ja Suomen Asianajajaliitosta.¹⁹

Hallituksen esityksessä todettiin, ettei kansallisessa lainsäädännössä ole säännöksiä, joiden voitaisiin katsoa kattavan 5 kohdassa tarkoitettut tilanteet. Kun kyseessä on identiteettivarkausrikos, on tyypillistä tutkinnan aikana kohdistaa epäilyt henkilöön, jonka identiteetti-, yksilöimis- tai tunnistamistietoja on käytetty rikoksessa. Velvoitteiden täyttämiseksi oli arvioitu useita vaihtoehtoja, ja hallituksen esityksessä oli kaikkien näiden vaihtoehtojen poissulkeminen perusteltu tarkasti. Hallituksen esityksen mukaan voitiin katsoa olevan kansallisten tarpeiden kannalta perusteltua panna täytäntöön 5 kohdan identiteettivarkauksiin liittyvät velvoitteet itsenäisellä kriminalisoinnilla, ja tämän johdosta päädyttiin esittämään lisättäväksi rikoslain 38 lukuun uusi 9 b §, joka vastaisi direktiivin määräyksiä rajautumatta kuitenkaan direktiivin 4 ja 5 artiklassa tarkoitettujen rikosten tilanteisiin.²⁰

Uuden pykälän tarkoituksena oli suojella identiteetin loukkaamattomuutta, toisin sanoen suojella henkilöä, jonka henkilötietoja on rikoksessa käytetty, ja samalla mahdollistaa tuomitseminen myös tietojärjestelmien ja datan suojelun ollessa tarpeen. Esityksessä huomioitiin myös, että käytettäessä hyväksi toisen henkilötietoja on mahdollisesti syyllistytty muun muassa rikoslain 36 luvun 1 §:ssä tarkoitettuun petokseen. Eroavaisuus identiteettivarkauden ja petoksen välillä onkin lähinnä suojeluobjektissa, joka petoksissa on erehdytettävän henkilön omaisuuden suoja, kun taas identiteettivarkauksissa kyseessä on jo aiemmin mainittu henkilön identiteetin loukkaamattomuus. Ehdotetun uudistuksen tarkoituksena oli keskittyä siihen henkilöön, jonka identiteettitietoja on käytetty väärin, ja jonka asemaa säännöksellä oli tarkoitus parantaa. Ehdotuksen taustalla oli myös se, ettei rajauduttaisi ainoastaan internet-ympäristöön tai televiestintään, koska tietojärjestelmiä ja tietoliikennettä on mahdollista häiritä ja dataa vahingoittaa myös fyysisin keinoin. Ehdotusta puolsi direktiiviin liittyvien vaatimusten täyttämisen ohella se, että kansallisella tasolla identiteettivarkauksien kriminalisointiin, varsinkin identiteettivarkauksien uhrin asemaan, oli alettu kiinnittää enemmän huomiota.²¹

¹⁸ HE 232/2014

¹⁹ OM 15/41/2013

²⁰ HE 232/2014

²¹ HE 232/2014

Hallituksen esitys laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräksi siihen liittyviksi laeiksi annettiin eduskunnan käsiteltäväksi 13.11.2014, ja hallituksen esitykseen liittyvä Lakivaliokunnan mietintö²² valmistui 27.2.2015. Eduskunnan ensimmäinen esitystä koskeva käsittely oli 4.3.2015, ja tällöin se hyväksyi esitykseen sisältyvät lakiehdotukset ja uuden lakiehdotuksen sellaisenaan. Toinen eduskunnan käsittely tapahtui 10.3.2015, ja tällöinkin eduskunta hyväksyi ensimmäisessä käsittelyssä sisällöltään päätetyt lakiehdotukset ja mietinnössä ehdotetun uuden lakiehdotuksen.²³ Eduskunta hyväksyi mietintöön sisältyvän lausumaehdotuksen, ja asian käsittely päättyi. EU:n asettaman määräajan mukaisesti laki astui voimaan 4. syyskuuta 2015 ainoastaan sillä muutoksella, että kyseessä oli rikoslain 38 luvun 9 a § eikä ehdotuksessa mainittu 9 b §.

2.2 Identiteettivarkauden muodot

Identiteettivarkaudesta puhuttaessa tarkoitetaan tekoa jossa rikoksen tekijä hankkii tietoonsa jonkun toisen henkilötietoja kuten nimen, sosiaaliturvatunnuksen, luottotiedot tai esimerkiksi salasanan sähköpostiin tai sosiaalisen median tileihin. Näitä tietoja tekijä pystyy käyttämään esiintyäkseen toisena henkilönä, jonka avulla tekijän on mahdollista tehdä useita erilaisia petoksia kuten ottaa lainaa, hallinnoida henkilön varoja tai käyttää hänen sosiaalista asemaansa hyväksi. Yksinkertaisemmin sanottuna identiteettivarkaudessa on useimmiten kyse toisen henkilötietojen ja maineen varastamisesta oman taloudellisen hyödyn vuoksi.²⁴ Identiteettivarkauksien voidaan yksinkertaistetusti katsoa jakautuvan kahteen eri ryhmään, perinteisempiin identiteettivarkauksiin ja verkossa tapahtuviin identiteettivarkauksiin.

Perinteisillä identiteettivarkauksilla tarkoitetaan tosielämässä tapahtuvaa henkilötodistuksen varastamista kuten passin, henkilökortin, luottokortin tai muun tiedon fyysistä varastamista henkilökohtaisten tunnistetietojen saamiseksi ja oman taloudellisen hyödyn saavuttamiseksi. Verkossa tapahtuvilla identiteettivarkauksilla taas tarkoitetaan niin sähköpostien, sosiaalisen median tilien kuin vaikkapa verkkopankkitunnusten varastamista vastaavasta syystä. Perinteisesti toteutettuja identiteettivarkauksiakin tapahtuu edelleen ja niissä tekijä esimerkiksi kaivaa lehtiroskiksista henkilötietoja sisältäviä asiakirjoja tai tilauslehtiä, varastaa postia tai kalastelee tietoja puhelimitse. Verkossa tapahtuvat identiteettivarkaudet taas ovat selkeästi kasvava riski, ja niissä tekijä usein esiintyy aidon organisaation nimellä sähköpostin tai nettisivujen avulla ja sitä kautta saa uhrin luovuttamaan esimerkiksi salasanojaan tai tilitietojään. Toinen verkossa tapahtuva identiteettivarkauden muoto on erilaiset virukset ja hakke-

²² LaVM 29/2014 vp

²³ Eduskunta, Tietoverkkorikosdirektiivin täytäntöönpano. Viitattu 12.7.2017

²⁴ Biegelman 2009, s. 2.

rintiohjelmat joilla tunkeudutaan uhrin tietokoneeseen varastamaan tietoja esimerkiksi näippäilytallennuksen kautta.²⁵

Hyvä kysymys onkin, kuinka identiteetti sitten oikein voidaan varastaa. Kuten jo aiemmin mainittu, voi tekijä kaivaa postilaatikoista tai lehtiroskiksista henkilötietoja sisältävää materiaalia, hakkeroida tietokoneita tai esiintyä jonkin organisaation nimellä. Näiden lisäksi on kuitenkin muitakin tapoja joilla toisen henkilötiedot voidaan saada haltuun. Muun muassa Yhdysvaltojen Oklahoman poliisilaitoksen internet-sivuilla on lueteltu useita eri tapoja joilla identiteettivarkaus voi mahdollisesti tapahtua. Tekijä voi esimerkiksi varastaa tiedot yrityksestä jossa uhri on asiakkaana, työntekijänä tai vaikkapa potilaana, seistä uhrin takana kassalla ja ottaa ylös saamansa henkilötiedot tai pankkikortin tunnusluvun, kopioida eli skimmata uhrin pankki- tai luottokortin automaatilla tai esiintyä auktoriteettina, kuten poliisina, ja saada uhrin vapaaehtoisesti luovuttamaan henkilötietojaan.²⁶

Identiteettivarkaus on mahdollista tehdä myös varastamalla lompakko tai laukku jossa on henkilötodistuksia tai pankkikortteja, varastamalla tietoja kotimurron yhteydessä tai käyttämällä uhrin internetissä jakamia tietoja.²⁷ Tekijä voi tämän jälkeen käyttää saamiaan tietoja kalliisiin ostoksiin jotka voi helposti myydä eteenpäin, avata luottotilejä uhrin nimiin, ottaa lainoja tai ostaa vaikkapa auton uhrin nimissä, hankkia puhelinliittymän uhrin nimiin tai tyhjentää pankkitilin.²⁸ Tapoja varastaa toisen identiteetti on siis paljon, ja uusia tapoja syntyy varsinkin verkossa varmasti jatkossakin. Uhrin kannalta tärkeässä roolissa onkin siis identiteettivarkauden mahdollisuuden tiedostaminen ja omien tietojensa mahdollisimman hyvä suojaus niin verkossa kuin arkielämässäkin.

2.3 Teon tarkoitukset

Identiteettivarkaudella on aina jokin päämäärä tai tavoite johon tekijä haluaa päästä. Useimmiten tämä päämäärä on jonkintasoinen rikos. Kuten jo aiemmin on mainittu, haluaa tekijä usein saavuttaa taloudellista hyötyä joko saamalla käyttöönsä identiteetin haltijan varat tai ottamalla hänen nimissään lainaa tai ostamalla irtainta omaisuutta. Tällöin tekijä valmistelee rikosta varastamalla uhrin tunnistetietoja kuten passin tai kirjautumistiedot, hyö-

²⁵ Artikkel, Norton, Merritt. Identiteettivarkauden välttäminen. Viitattu 20.7.2017

²⁶ OU Police department, internet safety, How identity thieves get your personal information. Viitattu 20.7.2017

²⁷ OU Police department, internet safety, other forms of old-fashioned fraud and theft. Viitattu 20.7.2017

²⁸ OU Police department, internet safety, How identity thieves use your personal information. Viitattu 20.7.2017

dyntääkseen näitä tietoja petoksen tai väärennöksen yhteydessä. Näitä tietoja tekijä voi käyttää myös maksuvälinepetoksissa, henkilörekisteririkoksissa sekä kunnian- tai yksityisyyden loukkaamiseen liittyvissä rikoksissa. Kun kyse on taloudellisen tai muun oman hyödyn tavoittelemisesta, on useimmiten kyseessä järjestäytynyt rikollisuus, vaikkakin jossain määrin myös yksittäiset henkilöt tekevät identiteettivarkauksia taloudellisen hyödyn saavuttamiseksi.²⁹

Toinen mahdollinen identiteettivarkauden päämäärä on uhriin kohdistuva kiusanteko jossa yleisimmin yhteisöpalveluihin luodaan profiili toisen henkilön nimellä tai varastetaan jo käytössä oleva profiili. Käytössä olevan profiilin varastaminen huomataan useimmiten melko pian, jolloin kiusanteko jää suhteellisen pieneksi, kun taas kokonaan uuden profiilin luominen voidaan huomata vasta paljon myöhemmin ja vahinkoa ehtii tapahtua mahdollisesti enemmänkin. Silloin kun väärinkäyttöön ei liity taloudellisen edun tavoittelu, on puuttuminen rikosoikeudellisin keinoin usein mahdotonta. Kun identiteettivarkaudella halutaan kiusata nimenomaista uhria, liittyy siihen mahdollisesti myös uhrin mustamaalaus ja läheisten ihmissuhteiden vahingoittaminen, uhrin maineen tai kunnian loukkaaminen tai yksityiselämää loukkaavan tiedon levitys. Tapauksissa joissa on jo selkeästi kyse jostakin edellä mainituista, on kyse vakavista rikoksista ja tällöin rikosoikeudellinen puuttuminen asiaan tulee mahdolliseksi. Näiden rikosten selvitys on kuitenkin usein ongelmallista, sillä tekijää voi olla vaikeaa saada selville jos on käytetty esimerkiksi julkisella paikalla sijaitsevaa konetta tai ulkomaalaista palvelinta.³⁰

Tiedossa on myös tapauksia joissa tekijä käyttää uhrin kuvaa, mutta esiintyy toisilla henkilötiedoilla. Tällöin tekijän tarkoitus on huijata jotakin kolmatta osapuolta tekeytymällä eri henkilöksi kuin kuka hän todellisuudessa on, kuitenkin käyttämättä uhrin todellista henkilöllisyyttä kuvan ohella. Tällaisissa tapauksissa tekijä saattaa esimerkiksi pyrkiä romanttiseen suhteeseen internetin välityksellä huijauksensa kohteen kanssa. Tekijä ei tällöin yleensä joko jostakin syystä kehtaa tai halua paljastaa todellista henkilöllisyyttään tai hän haluaa nimenomaisesti tehdä kiusaa valitsemalleen uhrille. Kyseiset huijaukset voivat kestää jopa useita vuosia, ja osa näistä tapauksista ei yhteydenpidon loputtua selviä välttämättä koskaan.³¹ Näihin tapauksiin voidaan laskea myös rikokset joissa tekijä esiintyy verkossa ikäistään nuorempana avatakseen keskustelua lapsen tai nuoren kanssa.³²

Kaikkien identiteettivarkautapausten kohdalla on ilmeistä, että uhriin kohdistuneilla väärinkäytöksillä loukataan hänen itsemääräämisoikeuttaan, yksityisyyttään ja mainetta tai kunni-

²⁹ Pesonen 2013, s. 145.

³⁰ Pesonen 2013, s. 146.

³¹ Pesonen 2013, s. 147.

³² Forss 2014, s. 95.

aansa sekä uhrin oikeutta omiin henkilötietoihinsa tai kuviinsa ja nimeensä. Tapaukset aiheuttavat uhrille harmia riippumatta siitä, onko kyseessä todellinen rikos tai onko tietoja käytetty loukkaamistarkoituksessa. Kun kyseessä ei ole perinteinen rikos, ei uhri myöskään välttämättä saa minkäänlaista suojaa ilkivaltaa vastaan riippumatta siitä, että perustuslakiinkin on kirjattu yksityiselämän, kunnian ja henkilötietojen suoja. Onkin väistämättä palveluntarjoajan vastuulla poistaa vääräksi ilmoitetut profiilit riippumatta siitä, onko niillä tehty rikollisia toimia. Myös yhä yleistyvä pelko on, että eri palveluntarjoajien keräämät ja usein julkisetkin profiilitiedot mahdollistavat identiteettivarkaille entistä helpomman tavan kerätä henkilötietoja laittomaan ja jopa rikolliseen toimintaan.³³ Kun tarkastellaan aiemmin mainittuja identiteettivarkauden tekokeinoja, ei tämä pelko kovinkaan kaukaa haetulta vaikutakaan.

2.4 Rangaistavuus ja mahdolliset rikosnimikkeet ennen kriminalisointia

Ennen vuotta 2015 identiteettivarkautta ei sellaisenaan ollut kansallisessa lainsäädännössä kriminalisoitu, joten identiteettivarkautapauksissa tekijää oli syytettävä muilla rikosnimikkeillä mikäli siihen oli mahdollisuus. Yleisimmin sosiaalisessa mediassa tapahtuvissa identiteettivarkauksissa rikosnimikkeenä oli kunnianloukkaus³⁴ tai yksityiselämää loukkaavan tiedon levittäminen³⁵, joiden motiivina oli kiusaaminen. Esimerkiksi valeprofiileista tuli ilmoituksia nettipoliisille lähes päivittäin jo ennen identiteettivarkauden kriminalisointia. Toinen mahdollinen rikosnimike oli tietomurto³⁶, joka voitiin jakaa kahteen eri tekemuotoon. Ensimmäinen näistä muodoista on tietojärjestelmään murtautuminen, niin sanottu tietokonerauhan rikkominen. Toinen muoto taas on tietojärjestelmän yksityisyyden loukkaaminen jossa ei ole kysymys salakuuntelusta tai -katselusta. Tällöin on kyse siitä, että tekijä on tunkeutunut tietojärjestelmään tai sen osaan, johon hänellä ei ole minkäänlaista oikeutta päästä. Kyseisissä tapauksissa rangaistavuuden edellytyksenä oli, että tekijä mursi järjestelmän turvajärjestelyn.³⁷

Ennen identiteettivarkauden kriminalisointia voitiin tekijää syyttää myös viestintäsalaisuuden loukkauksesta³⁸, mikäli tekijä oli päässyt käsiksi uhrin sähköposteihin tai sosiaalisen median tileihin joissa oli mahdollisuus yksityisviesteihin muiden käyttäjien kanssa. Muutamissa tapauksissa käräjäoikeus on myös ennen kriminalisointia tuominnut toisen henkilön sosiaalisen median tilin käyttämisen luvattomana käyttönä³⁹. Ratkaisuja voidaan kuitenkin pitää kritiikille

³³ Pesonen 2013, s. 147-148.

³⁴ RL 24:9

³⁵ RL 24:8

³⁶ RL 38:8

³⁷ Forss 2014, s. 242-244.

³⁸ RL 38:3

³⁹ RL 28:7

avoimena ellei kirjautuminen ole tapahtunut nimenomaisesti uhrin omalta tietokoneelta, vaikka sillä ei ole väliä, onko koneelle kirjaututtu paikan päältä vai etäyhteyden kautta. Toisin sanoen jos tekijä on kirjautunut toisen henkilön sosiaalisen median tilille, vaikkapa Facebookiin, muun kuin uhrin oman koneen kautta, olisi asianomistajana tällöin Facebook eikä käyttäjätilin haltija.⁴⁰

Identiteettivarkauksista oli ennen kriminalisointia mahdollista tuomita myös henkilörekisteririkoksesta⁴¹, mutta kyseisellä rikosnimikkeellä tunnusmerkistön täyttymisen todistaminen oli ajoittain melko ongelmallista. Henkilötiedot on jo Suomen perustuslaissakin laskettu kuuluvaksi yksityiselämän suojaan⁴² sekä henkilötietojen suojaan⁴³ ja tarkoituksena on ollut nimenomaisesti turvata yksilön oikeusturvaa sekä yksityisyyden suojaa henkilötietoja käsiteltäessä, rekisteröitäessä ja käytettäessä. Henkilörekisteririkoksen tunnusmerkistössä mainittu henkilötietolaki on kuitenkin valitettavan paljon aikaansa jäljessä, ja sitä on tästä syystä ollut vaikeaa soveltaa sosiaalisen median yhteydessä. Jos henkilötietolakia lähdettäisiin sosiaalisen median yhteydessä vahvemmin soveltamaan, tulisi myös jokainen kuva jossa esiintyy toinen henkilö ilman omaa suostumustaan tulkita henkilötietolain vastaiseksi. Henkilörekisteririkos onkin ennen identiteettivarkauden kriminalisointia ollut ajankohtainen rikosnimike lähinnä perinteisissä identiteettivarkauksissa joissa teko ei ole tapahtunut verkossa tai sosiaalisessa mediassa. Rikoslain henkilörekisteririkoksen ohella on olemassa lievempi tekemuoto, henkilörekisteririkkomus⁴⁴, ja käytännössä kaikissa sosiaalisessa mediaan liittyvissä identiteettivarkauksissa olisi tulkittavissa korkeintaan jälkimmäinen.⁴⁵ Henkilötietolaki tullaan kuitenkin siinä mielessä päivittämään nykyaikaisemmaksi, että 25.5.2018 alkaen sovellettavaksi tulee Euroopan parlamentin ja neuvoston niin kutsuttu tietosuojasetus,⁴⁶ joka kumoaa voimaantulollaan tietosuojan nykyiset yleissäädökset, juurikin kansallisen henkilötietolain sekä EU:n henkilötiedodirektiivin.⁴⁷

⁴⁰ Forss 2014, s. 245-250.

⁴¹ RL 38:9

⁴² PL 2:10

⁴³ HeTiL 523/1999.

⁴⁴ HeTiL 10:48

⁴⁵ Forss 2014, s. 250-252.

⁴⁶ EU 2016/679, Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojeleminen henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta.

⁴⁷ Lång & Tolvanen 2016, s. 5.

Vakavammissa identiteettivarkaustapauksissa oli rikosnimikkeenä ennen lainuudistusta ja kriminalisointia yleisimmin jonkinasteinen petos⁴⁸. Jos siis pystyttiin katsomaan tekijän hankkineen taloudellista hyötyä erehdyttämällä tai erehdystä hyväksi käyttämällä, voitiin hänen katsoa syyllistyneen petokseen. Petoksesta pystyttiin tuomitsemaan niin perinteisissä kuin verkossa tapahtuvissa identiteettivarkaustapauksissa mikäli tekijä oli hankkinut teolla itselleen taloudellista hyötyä jollakin tapaa. Petoksessa niin hyötymistarkoituksessa kuin vahingoittamistarkoituksessakin tehty rikos ovat rangaistavissa. Myös verkkopankkiin liittyvien rikosten kohdalla oli mahdollista käyttää rikosnimikkeenä petosta, mutta perinteiselle identiteettivarkaudelle ominaisessa luotto- tai pankkikortin väärinkäytössä katsotaan aina kyseessä olevan maksuvälinepetos⁴⁹. Ero näiden kahden välillä on siinä, ettei verkkopankkitunnusten katsota olevan itsessään maksuväline, kuten vaikkapa luottokortti taas on. Petoksessa myös yritys on rangaistava, joten jos identiteettivarkauden yritys on voitu näyttää toteen, mutta taloudellista hyötyä ei ole tekijälle ehtinyt kertyä, on hänet voitu tuomita petoksen yrityksestä.⁵⁰

Vuoteen 1999 asti Suomen kansallisessa lainsäädännössä oli kriminalisoitu yksityishenkilön erehdyttäminen jos teossa käytettiin toisen henkilön passia, työtodistusta tai muuta vastaavaa todistusta. Säännös päädyttiin kuitenkin poistamaan lainsäädännöstä koska kyseisten tekemuotojen katsottiin liittyvän yleensä muiden rikosten tunnusmerkistöön. Vuonna 2006 rikoslakia uudistettaessa ehdotettiin samankaltaisen säännöksen lisäystä lakiin, mutta lakivaliokunta ei katsonut kriminalisoinnille olevan riittäviä perusteita. Kun identiteettivarkautta itsessään ei vielä ollut kriminalisoitu, oli rikosoikeudellisesti melko hankalaa varsinkin sosiaalisen median ja siellä tapahtuvien identiteettivarkauksien yleistyessä yrittää löytää rikosnimikettä jonka tunnusmerkistöön rikos saattaisi sopia. Jos identiteettivarkaudessa täytyikin esimerkiksi kunnianloukkauksen tunnusmerkistö, oli teko itsessään kuitenkin melko kaukana pykälän nimenomaisesta ydinalueesta. Kriminalisoinnin tarve on ollut selkeä siitä asti kun digitaaliset tietoverkot ovat yleistyneet, ja varsinkin sosiaalisen median kautta tekojen määrä on ollut räjähdysmäisessä ja jatkuvassa nousussa. Vaikka vuoden 2015 lainuudistuksen myötä identiteettivarkaus kriminalisoitiin ja kriminalisointi itsessään kattoi laajan kirjon henkilötietoja suojansa piiriin, jäi uudistukseen myös huomattavia aukkoja ja epäkohtia. Kriminalisoinnin mukaisesti sen lisäksi, että kolmannen osapuolen tulisi erehtyä, tulee teolla aiheuttaa myös taloudellista vahinkoa tai vähäistä suurempaa haittaa uhrille. Kriminalisoinnilla ei siis välttämättä lisätty mahdollisuuksia sosiaalisen median identiteettivarkauksiin puuttumiseen

⁴⁸ RL 36:1

⁴⁹ RL 37:8

⁵⁰ Forss 2014, s. 253-256.

ja suurena mahdollisuutena on, että valtaosa tapauksista tullaan syyttäjän toimesta rajoittamaan samalla tavalla kuin kunnianloukkausten kohdalla nykyisin.⁵¹

3 Identiteettivarkauden uhri

Identiteettivarkaalte kelpaa yleisesti ottaen mikä tahansa helposti saatavilla oleva tieto, minä johdosta uhriksi voi joutua periaatteessa kuka vain. Perinteisten identiteettivarkauksien uhriksi voi joutua missä vain, jos tilanteeseen ei osaa varautua tai tietojaan käyttää tai esittele huolimattomasti. Nykyisin yleisempien, verkossa tapahtuvien identiteettivarkauksien uhriksi taas voi joutua herkemmin jos tietokoneen turvallisuus ei ole ajantasaista tai jos jakaa liian huolimattomasti henkilötietojaan sosiaalisiin medioihin tai muille verkkosivuille.⁵² Mitä kokemattomampi verkon käyttäjä uhri on, sitä läpinäkyvämpien rikosten uhriksi hänen on todennäköistä joutua. Toisaalta taas verkkorikosten uhriksi joutumisen suurin riski on niillä jotka käyttävät useita palveluita tai viettävät paljon aikaa internetissä. Myös henkilön internetkäyttäytyminen vaikuttaa uhriksi joutumiseen, ja yleisimmin uhri onkin aktiivisesti eri palveluita käyttävä henkilö.⁵³

Kaikki verkkoa käyttävät henkilöt eivät pidä tietokoneensa virusturvaa ajan tasalla ja harva suojaa henkilökohtaista konettaan salasanalla. Jos siis internetyhteys on jatkuvasti auki eikä konetta ole asianmukaisesti suojattu, on esimerkiksi haittaohjelmien asennus suhteellisen helppoa osaavalle tekijälle. Verkossa tapahtuukin täysin samoja rikoksia kuin tosimaailmassa, ne on vain helpompaa toteuttaa huomaamatta ja kiinni jäämättä, koska rikoksen voi tehdä verkossa myös esimerkiksi toisesta maasta käsin.⁵⁴ Jos henkilö esimerkiksi levittää tarpeettomasti henkilötietojaan julkisesti sosiaalisessa mediassa, antaa arkaluontoisia tietojaan sivustoille joita ei ole kunnolla salattu tai käyttää yksinkertaisia ja helppoja salasanoja, on hänen todennäköisempää joutua jossakin vaiheessa identiteettivarkauden uhriksi.⁵⁵

Identiteettivarkaat hankkivat uhriensa tietoja usein myös niin sanotuin perinteisin keinoin kuten kaivamalla lehtiroskiksista henkilötietoja sisältäviä asiakirjoja, varastamalla postia, skimmaamalla pankkikortin automaatilla tai varastamalla lompakon. Jos siis henkilö heittää huolimattomasti pois henkilötietojaan sisältäviä asiakirjoja silppuamatta tai muuten tuhoamatta niiden sisältämät henkilötiedot, jättää vaikkapa autoon näkyville lompakkonsa poistessaan tai ei suojaa korttinsa koodia asioidessaan liikkeissä, on hänen todennäköisempää joutua

⁵¹ Forss 2014, s. 86-89.

⁵² Poliisi. Tietoverkkorikoksia. Viitattu 27.7.2017

⁵³ Haasio 2013, s. 14.

⁵⁴ Haasio 2013, s. 13-14.

⁵⁵ Haasio 2013, s. 47.

tua identiteettivarkauden uhriksi.⁵⁶ Vaikka mahdollisuus identiteettivarkauden uhriksi joutumiselle onkin aina olemassa, voi todennäköisyyttä vähentää toimimalla huolellisesti niin verkossa kuin arkielämässään. Jos tekijälle aukeaa tilaisuus, hän tuskin sitä jättää käyttämättä, ja tästä syystä mahdollisen uhrin oma toiminta onkin ennaltaehkäisyn avainasemassa. Kun identiteettivarkaus on ehtinyt tapahtua, on uhrin pystyttävä se todistamaan ja turvattava mahdollisimman hyvin henkilötietonsa ja kohdattava mahdolliset seuraukset niin sosiaalisessa kuin taloudellisessakin mielessä. Koska identiteettivarkaus omana rikosnimikkeenä on edelleen varsin tuore, on myös ennakkotapauksia vielä verrattain vähän ja uhrin voi olla vaikeaa löytää tarpeelliset tiedot rikoksen selvittämiseksi.

3.1 Uhrin asema identiteettivarkauksissa

Kansainvälisessä vertailussa uhrin asema rikostapauksissa on Suomessa suhteellisen hyvällä tasolla, sillä uhrilla on oikeusprosessin osalta suhteellisen vahva rooli asianomistajana ja hänen on mahdollista toimia oikeudenkäynnissä todistajana, jolloin hänen todistuksensa on yhtä pätevä ja todistusvoimainen kuin kenen vain asiassa todistavan tahon. Uhrilla on oikeus yhtyä syytevaatimukseen syyttäjän kanssa sekä vaatia syytettä esimerkiksi törkeästä petoksesta jos syyttäjä esittää syytettä lievästä petoksesta, ja lisäksi uhri voi käyttää toissijaista syyteoikeuttaan jos syyttäjä jättää syytteen nostamatta. Myös rikosvahinkojen korvausjärjestelmää on kehitetty erityisen pitkälle, ja uhrin on mahdollista saada korvauksia esimerkiksi valtion varoista Valtionkonttorin kautta. Uhri voi myös hakea mahdollisia vahingonkorvauksia rikosoikeudenkäyntinsä yhteydessä eikä hänen tarvitse käydä läpi erillistä käsittelyä siviilioikeudessa, ja selvissä tapauksissa syyttäjä voi suoraan ajaa asianomistajan vahingonkorvausvaatimusta.⁵⁷

Identiteettivarkauksissa on kyse asianomistajarikoksista, joten rikoksen selvittämiseksi uhrin on itse tehtävä poliisille tutkintapyyntö. Vaikka kyseessä olisi identiteettivarkaus jonka seuraukset ovat olleet verrattain pienet, kannattaa uhrin aina tehdä tutkintapyyntö. Jos identiteettivarkauden rikosnimikkeen vaatimat lainkohdat eivät täyty, voi kyseessä olla kuitenkin esimerkiksi yksityiselämää loukkaavan tiedon levittäminen, kunnianloukkaus tai petos. Joissakin tapauksissa uhri ei välttämättä edes ymmärrä kyseessä todella olevan identiteettivarkaus jos seuraukset ovat suhteellisen pieniä tai olemattomia. Kuitenkin näissäkään tapauksissa toinen henkilö on saanut käyttöönsä uhrin henkilötietoja ja hän voi myöhemmin käyttää niitä vakavampiin, rikollisiin tarkoituksiin. Uhri voi myös kokea, ettei lievä taloudellinen menetys ole riittävän painava syy tehdä ilmoitusta tai ettei tapauksesta ilmoittaminen ole vaivan ar-

⁵⁶ Haasio 2013, s. 47.

⁵⁷ Kjällman 2011, s. 13.

voista.⁵⁸ Tällaisia tapauksia voivat olla esimerkiksi verkkopankkitunnusten saaminen, mutta tekijä ei ehdi saada pankkisiirtoaan läpi, jos uhri ehtii sulkea tilinsä.

Kun henkilö huomaa joutuneensa identiteettivarkauden uhriksi, on hänen mahdollista asettaa itselleen kahden vuoden määräaikainen luottokielto vahinkojen minimalisoimiseksi. Uhri voi myös varmistaa osoitetietojensa oikeellisuuden väestörekisterikeskuksesta, maistraatista tai postista sekä tarvittaessa oikaista tiedot ja ilmoittaa henkilötietojensa väärinkäytöstä. Jos kyseessä on maksukorttiin tai pankkitunnuksiin liittyvä identiteettivarkaus, on verkkopankkitunnukset tai maksukortti suljettava välittömästi ja pankille ilmoitettava väärinkäytöstä. Jos maksu on tapahtunut kolmannen osapuolen maksupalvelussa kuten PayPalissa, on uhrin ilmoitettava palveluntarjoajalle asiasta ja vaadittava maksun kumoamista. Sosiaalisessa mediassa uhri voi pyytää valeprofiilien poistoa palveluista, ja salasanat tulisi aina vaihtaa kun verkossa on tehty identiteettivarkausrikos. Salasanaa vaihdettaessa palautussähköpostiosoite tulisi tarkistaa, ja tilin palautukseen on mahdollista saada palveluntarjoajan apua tarvittaessa. Jos palvelussa on mahdollista nähdä oma kirjautumishistoriansa, kannattaa myös se tarkistaa ja kaikki muut aktiiviset kirjautumiset tulee tällöin sulkea ja mahdollisuuksien mukaan ottaa käyttöön vahva tunnistus.⁵⁹

Koska uhrin on pystyttävä todistamaan rikosilmoituksen yhteydessä identiteettivarkauden tapahtuneen, on kaikesta kerättävä todisteita ja tietoja. Jos kyseessä on maksukorttiin, maksupalveluntarjoajaan tai verkkopankkitunnuksiin liittyvä rikos, tulee uhrin kerätä kaikki luvattomiin maksutapahtumiin liittyvät tiedot rikosilmoitusta varten vaikka pankki tai maksupalveluntarjoaja ehtisikin oikaista tapahtuneen ennen kuin vahinko todella ehtii tapahtua. Jos kyseessä on sosiaalisessa mediassa tai muualla verkossa tapahtuva valeprofiili tai muu identiteettivarkaus, kannattaa todisteita kerätä esimerkiksi ruutukaappauksin. Jos taas kyseessä on identiteettivarkaus jossa uhrin tiedoilla on tilattu verkossa omaisuutta, todisteiksi kannattaa kerätä esimerkiksi tilausvahvistukset tai maksuihin liittyvät perintäkirjeet tai maksukehotukset. Viimeksi mainituissa tapauksissa on poliisin lisäksi tärkeää olla yhteydessä petoksen kohteena oleviin organisaatioihin tai kauppiaisiin ja tarvittaessa tilauksista on tehtävä reklamaatio.⁶⁰ Jotta uhrille aiheutuvat haitat pysyisivät mahdollisimman pieninä, on uhrin toimittava nopeasti huomattuaan identiteettivarkauden tapahtuneen. Jos uhri ei toimi nopeasti, on vaarana suurempi taloudellinen menetys, tai esimerkiksi sosiaalisen median valeprofiilien kohdalla tekijä saattaa ehtiä poistamaan todisteet, jos epäilee uhrin olevan tietoinen rikoksesta.

⁵⁸ Kjällman 2011, s. 14-15.

⁵⁹ Rikosuhripäivystys 2014. Viitattu 27.7.2017

⁶⁰ Rikosuhripäivystys 2014. Viitattu 27.7.2017

3.2 Vaikutukset uhriin

Uhrin kannalta yksinkertaisten henkilötietojenkin avulla aikaansaattavan haitan vuoksi on tärkeää tarkastella myös, mihin kaikkeen identiteetin varastaminen vaikuttaa. Yksilön henkilötietojen suojan ja tietosuojan yhteydessä voidaan mainita suora yhteys intimitettisuojaan, salassapidon, yksityisyyden ja yksityiselämän suojaan sekä itsemääräämisoikeuden käsitteisiin, niin sanottuun henkilöoikeuteen. Henkilöoikeutta voidaan jakaa kahteen osa-alueeseen, materiaaliseen ja muodolliseen henkilöoikeuteen. Materiaalisesta henkilöoikeudesta puhuttaessa tarkoitetaan henkilön oikeuksia ja yhteiskunnan henkilöä suojaavia säädöksiä, niin sanottuja suojasäännöksiä. Materiaalisen henkilöoikeuden kautta voidaan tutkia esimerkiksi henkilön yksityisyyttä, tietosuojaa ja tasa-arvoa. Muodollisen henkilöoikeuden kohdalla taas tarkoitetaan oikeussubjektin eksistenssiä, alkuperää sekä suhdetta muihin oikeussubjekteihin ja niiden tunnistusta, vastuuta ja päättymistä. Tätä kautta voidaan tutkia oikeuskelpoisuutta ja oikeustoimikelpoisuutta. Henkilöoikeuden keskeisimpänä näkökohtana onkin yksilön kunnioittaminen ja lähemmin tarkasteltuna voidaan sen alta löytää itsemääräämisoikeus, yksityisyys ja yksilöllisyys.⁶¹

Kun yksityisyydestä puhutaan periaatteena, voidaan sen arvostusta pitää suorana yhteytenä ajatukseen kansalaisen perusoikeuksien kunnioituksesta. Määritelmänä yksityisyys on vaikeaa määrittää, ja esimerkiksi suomalaisessa lainsäädännössä yksityisyys mainitaan lähinnä käsitteen tasolla. Oikeutenakin yksityisyys on melko suhteellista ja se voi olla ajoittain toissijainen tärkeämmille yhteiskunnallisille tavoitteille. Yksityisyyteen voidaan katsoa kuuluvan henkilön oikeus saada tietoa ja pystyä päättämään itseään koskevien tietojen käytöstä, ja sitä voidaan pitää laajempänä kokonaisuutena yksityiselämän suojasta. Oikeudellisessa kirjallisuudessa yksityisyyttä on myös pyritty määrittelemään niin, että se olisi henkilötietojen kontrollia, ja itsemääräämisoikeuden näkökulmasta taas henkilön oikeus nimeensä, kuvaansa ja hahmoonsa, niin sanottu tiedollinen omistusoikeus.⁶² Kun siis henkilö joutuu identiteettivarkauden uhriksi, vaikuttaa rikos lähes poikkeuksetta hänen kykyynsä päättää itseään koskevien tietojen käytöstä tai henkilötietojensa kontrollista, ja tällöin loukataan myös henkilön tiedollista omistusoikeutta. Tällöin siis loukataan väistämättä uhrin yksityisyyttä ja hänen yksityisyyden suojaansa vaikkei teolla tavoiteltaisikaan rikoslain mukaisesti taloudellista hyötyä.

Yksityisyyden suoja on kansallinen perustuslaissa turvattu perusoikeus joka takaa henkilölle oikeuden tietää ja päättää itseään koskevista tietojen käytöstä, oikeuden olla yksin ilman häirintää, oikeuden henkilötietojen ja henkilösuhteiden kontrollointiin sekä itsemääräämisoikeuden. Yksityisyyden suojaan liittyy näiden lisäksi muita yksittäisiä perusoikeuksia, kuten oikeus

⁶¹ Korhonen 2003, s. 72-54.

⁶² Korhonen 2003, s. 74-79.

henkilökohtaiseen vapauteen, kunniaan ja yhdenvertaiseen kohteluun. Rikoslaisissa on kriminalisoitu yksityiselämää loukkaavan tiedon levittäminen, jolla osaltaan on haluttu varmistaa henkilön yksityisyyden suojaa.⁶³ Rikoslain lisäksi yksityisyyden suojaan vaikuttaa henkilötietolaki⁶⁴, laki viranomaisten toiminnan julkisuudesta⁶⁵, laki yksityisyyden suojasta työelämässä⁶⁶, tietoyhteiskuntakaari⁶⁷ sekä EU:n direktiiveistä henkilötietodirektiivi⁶⁸ ja sähköisen viestinnän tietosuojadirektiivi⁶⁹.⁷⁰

Yksityisyyden synonyymiksi mielletään nykyisin usein identiteetti tai henkilöllisyys. Ennen yksityisyydestä puhuttaessa on tarkoitettu sitä, etteivät kaikki asiat ole julkisia ja henkilön elämä on nähty osiltaan erilaisena kuin valtion viralliset tai julkiset asiat. Kuitenkin termejä identiteetti ja henkilöllisyys olisi ehkä sopivampaa käyttää digitaalisessa maailmassa nykyaikaisia haasteita tarkasteltaessa, ja pitää yksityisyyden termi ennemminkin arkiseen elämään kytkettynä. Identiteetti itsessään on alkujaan latinankielinen termi, jolla on tarkoitettu, että henkilö todella on se joksi häntä kuvataan tai hänen sanotaan olevan. Yksityiselämää voidaan nykyään suojella juurikin kontrolloimalla omaa identiteettiä. Siinä missä esimerkiksi henkilötiedot on ennen näytetty tai annettu vain henkilöille joilla on oikeus niiden näkemiseen ja käsittelyyn, saatetaan ne nykyisin verkossa tietämättään antaa kenelle tahansa, jos vain henkilöllä on tekniset resurssit saada tiedot käyttöönsä.⁷¹ Identiteettivarkauksia tarkasteltaessa yksityisyyden suojan rooli tulee siis esiin juuri siinä, että henkilön oikeutta tietojensa ja suhteidensa kontrollointiin sekä hänen kunniaansa on loukattu.

Toinen tärkeä perusoikeus, jota tässä yhteydessä on tarkasteltava, on henkilötietojen suoja. Henkilötietojen suoja linkittyy myös suoraan henkilön tiedolliseen itsemääräämisoikeuteen ja myös sitä sääntelevät kansallisen lainsäädännön ohella EU:n henkilötieto- ja sähköisen viestinnän tietosuojadirektiivit, jotka tosin nekin on kansallisessa lainsäädännössä huomioitu.⁷² Henkilötiedoilla tarkoitetaan kaikkia niitä luonnollista henkilöä, hänen elinolosuhteitaan tai omaisuuttaan kuvaavia merkintöjä, joiden avulla henkilö voidaan tunnistaa. Yksinkertaisimmillaan henkilötiedon voidaan ajatella olevan esimerkiksi henkilötunnus tai sormenjälki, sillä

⁶³ Pesonen 2013, s. 60-61.

⁶⁴ HeTiL 523/1999.

⁶⁵ JulKL 621/1999.

⁶⁶ YksTL 759/2004.

⁶⁷ TYK 917/2014.

⁶⁸ 46/1995/EY

⁶⁹ 58/2002/EY

⁷⁰ Viljanen 2013-2017, Viitattu 26.7.2017

⁷¹ Tranberg & Heuer 2013, s. 22-23.

⁷² Tranberg & Heuer 2013, s. 72-73.

molemmat voidaan selkeästi tunnistaa tiettyä henkilöä koskeviksi tiedoiksi. Laajemmin taas voidaan henkilötiedoiksi katsoa esimerkiksi tietokoneen IP-osoite, sähköpostiosoite tai ajoneuvon rekisterikilpi. Jotta jokin tieto voidaan luokitella henkilötiedoksi, on yksittäisen henkilön oltava tiedon perusteella tunnistettavissa.⁷³ Henkilötietojen suojalla rajoitetaan yksityishenkilön tietojen keräystä ja käsittelyä ja henkilöllä tulee olla tietoihinsa liittyen tarkastus-, korjaus- ja kiello-oikeus. Esimerkiksi sosiaalinen media kokonaisuudessaan perustuu nimenomaisesti sitä käyttävien henkilöiden henkilötietojen käsittelyyn, ja palveluntarjoajalle syntyy tämän seurauksena käyttäjistään erilaisia henkilörekistereitä joissa saatetaan säilyttää jopa käyttäjään liittyvää arkaluontoista tietoa.⁷⁴ Henkilön joutuessa identiteettivarkauden uhriksi käytetään siis hänen henkilötietojaan toisen henkilön toimesta, ja tällöin voidaan katsoa rikoksen loukkaavan myös uhrin henkilötietojen suojaa.

Kuten mikä tahansa rikos, myös identiteettivarkaus väistämättä yllättää uhrin. Vaikka uhri suojaisi identiteettiään asianmukaisin keinoin, voi rikos osua hänen kohdalleen varautumisesta huolimatta, ja uhriksi joutuminen voi järkyttää. Rikoksen uhri kokee lähes aina rikoksen jälkeen turvattomuuden tunnetta, ja tämän johdosta uhri reagoi jollakin tapaa tapahtuneeseen. Uhrin itsensä lisäksi rikos vaikuttaa hänen läheisiinsä, ystäviinsä sekä mahdollisesti työtovereihinsa. Myös rikoksen laajuus vaikuttaa uhrin reaktioon, ja tätä voidaan havainnollistaa esimerkiksi sillä, että yksittäinen identiteetin väärinkäyttö vaikuttaa uhriin vähemmän kuin vaikkapa vuosia jatkunut tai muuten toistuva identiteetin väärinkäyttö.⁷⁵ Jos siis esimerkiksi identiteettivarkauden uhrin nimissä tilataan verkkokaupasta kerran tuotteita, on tällä pienempi vaikutus uhriin kuin esimerkiksi sillä, että hänen nimissään on otettu lainoja, tilattu useaan otteeseen omaisuutta ja avattu puhelinliittymiä. Uhrille aiheutuvien juridisten seurausten lisäksi identiteettivarkaudesta seuraa uhrille psyykkisiä vaikutuksia sekä eritasoisia taloudellisia vaikutuksia, ja identiteettivarkauden luonteesta ja laajuudesta riippuen myös mahdollisia sosiaalisia vaikutuksia. Osaltaan myös nämä seuraukset vaikuttavat uhrin psyykkiseen reaktioon.

3.2.1 Sosiaaliset seuraukset

Yksityiselämää pidetään usein itsestäänselvyytenä kunnes sen syystä tai toisesta menettää. Yksityisyys on pohjimmiltaan mahdollisuus päättää itse mitä tietoja, milloin ja missä yhteyksissä henkilö tahtoo muille jakaa.⁷⁶ Jos haluaa vahingoittaa toista henkilöä ja tämän mainetta, on se etenkin verkossa todella helppoa. Toista henkilöä koskevaa informaatiota on helppo

⁷³ Vanto 2011, s. 22-23.

⁷⁴ Pesonen 2013, s. 89-91.

⁷⁵ Kjällman 2011, s. 19.

⁷⁶ Tranberg & Heuer 2013, s. 21.

vääristellä ja irrottaa asiayhteydestä, ja jälkeensä vääristettyä informaatiota voi olla uhrin toimesta hankalaa oikaista tai vahinkoa on jo voinut ehtiä tapahtumaan.⁷⁷ Uhrin identiteetillä voidaan tehdä muun muassa valeprofiili sosiaaliseen mediaan, jonka kautta tekijä voi olla hyvinkin aktiivinen. Uhrin on tämän jälkeen oikaistava kaikille asianosaisille kyseessä olleen valeprofiili, ja tämä saattaa aiheuttaa haittaa uhrin ihmissuhteissa tai pahimmissa tapauksissa jopa rikkoa ihmissuhteita. Jos taas uhrin nimissä on julkaistu loukkaavaa tai uhkaavaa sisältöä, esimerkiksi rasistisia tai toista henkilöä halventavia kirjoituksia, saattaa tämä aiheuttaa vahinkoa tai kärsimystä kirjoitusten kohteelle tai aiheuttaa uhriin itseensä kohdistuvaa syrjintää tai halveksuntaa, mitkä ovat jälleen omiaan vaikuttamaan uhrin sosiaalisiin suhteisiin.⁷⁸

Uhrin sosiaalisiin suhteisiin voivat myös vaikuttaa identiteettivarkauden seurauksena aiheutunut työpaikan vaihtuminen tai työttömyys, asuinpaikan vaihto tai harrastuksen päättyminen, tai osa sosiaalisista suhteista voi kokonaisuudessaan katketa näiden seurausten johdosta. Uusien sosiaalisten verkostojen luonti on aina hankalaa, ja rikoksen uhri saattaa lisäksi vältellä uusia ihmissuhteita, joka voi johtaa uhrin eristäytymiseen.⁷⁹ Identiteettivarkauden tekijä voi myös mahdollisesti olla uhrille entuudestaan tuttu tai läheinen henkilö, jolloin uhri tulee paitisi petetyksi ja menettää ihmissuhteen ja luottamuksen tekijään, on hänen myös entistä vaikeampi luottaa lähipiiriinsä rikoksen jälkeen. Rikos voi myös herättää uhrin lähipiirissä turvatomuuden tunnetta kun mahdollisuus rikoksen uhriksi joutumisesta konkretisoituu ja tuntuu mahdollisesti todennäköisemmältä kuin aiemmin. Uhrin sosiaaliset suhteet saattavat tämän seurauksena muuttua myös sisällöllisesti, kun lähipiiri joko tarjoaa apuaan ja tukeaan liiallisesti, utelee tapahtuneesta tai ei vain ymmärrä uhrin läpikäymiä tunteita ja reaktioita, ja tästä syystä ihmissuhteet etääntyvät.⁸⁰

Kun henkilö joutuu rikoksen uhriksi, ei hän välttämättä jaksa kiinnostua arkisista asioista tai ylläpitää niihin liittyviä keskusteluja. Uhrin käytös voi olla arvaamatonta ja sosiaalinen vuorovaikutus voi ontua tai olla lähes olematonta. Uhri ei välttämättä halua keskustella tapahtuneesta ja välttelee aihetta, kun taas lähipiiri on utelias tai haluaa auttaa ja tästä syystä koittavat saada uhria puhumaan tapahtuneesta tai ottavat sen itse jatkuvasti puheeksi uhrin aikana. Toisaalta taas uhri voi itse kokea suurta tarvetta puhua tapahtuneesta, joka saattaa aiheuttaa hämmennystä tai kyllästymistä lähipiirissä ja johtaa siihen, että he alkavat vähätellä tapahtunutta tai syyttää tai vältellä uhria.⁸¹ Omalta osaltaan kaikki nämä ovat identiteettivarkauden sosiaalisia seurauksia uhrin elämään, ja uhri voi kärsiä niistä vielä vuosia rikoksen

⁷⁷ Tranberg & Heuer 2013, s. 90-91.

⁷⁸ Forss 2014, s. 89; 94.

⁷⁹ Kjällman 2011, s. 37.

⁸⁰ Kjällman 2011, s. 36-37.

⁸¹ Kjällman 2011, s. 36.

selviämisen jälkeenkin. Osa ihmissuhteista voi päättyä kokonaan, osa saattaa etääntyä. Ihmissuhteiden lisäksi uhri voi menettää tietyissä piireissä maineensa kokonaan tai hänen maineensa voi huonontua ja uhri voi mahdollisesti menettää työnsä, luottamuksellisen tehtävän tai aseman tai harrastuksensa, ja hänen työnhakunsa tulevaisuudessa voi hankaloitua maineen tahriuduttua. Uhri saattaa myös jatkossa joutua selittelemään uusille tuttavuuksille tilannetta, mikäli identiteettivarkautta seuranneet tapahtumat ovat tulleet jollain tapaa yleiseen tietoon.

3.2.2 Taloudelliset seuraukset

Rikoksen nimikkeestä huolimatta uhrille aiheutuu lähes poikkeuksetta taloudellisia seurauksia. Rikos tulee kalliiksi paitsi yhteiskunnalle myös rikoksen uhrille itselleen. Vain harvoissa tapauksissa uhri saa todella täyden korvauksen menetyksiinsä nähden, joita rikoksesta riippuen voi tulla muun muassa varastetusta tai hajonneesta omaisuudesta, terveydellisistä tai oikeudenkäyntiin liittyvistä kuluista tai mahdollisesta ansionmenetyksestä. Uhrin on mahdollista vaatia tekijää maksamaan korvauksia aiheutuneista kuluista, mutta korvauksetkaan eivät yleensä kata kaikkia uhrille aiheutuneita menetyksiä tai kuluja, ja niiden saamisessa kestää suhteellisen kauan. Uhri ei myöskään huomaa välttämättä rikosilmoitusta tehdessään kaikkia aiheutuneita kuluja tai menetyksiä tai hän ei välttämättä vain tiedä, mistä kaikesta korvauksia on mahdollista hakea.⁸²

Rikoksesta voi aiheutua uhrille myös välillistä haittaa, kuten muutosta aiheutuneita kustannuksia tai yrittäjän elinkeinonmenetys ja mahdollisten yritysvelkojen takia seuraavat vaikeudet. Rikosta voi seurata myös työpaikan vaihto tai menetys tai työtehon merkittävä heikkeneminen hetkellisesti. Työtehon heikkeneminen voi myös hidastaa uhria etenemästä urallaan tai opinnoissaan, josta saattaa taas aiheutua välillistä taloudellista haittaa. Menetetyn omaisuuden ja oikeudenkäynnin johdosta aiheutuneiden kulujen hoitamiseksi uhri voi hakea vapaaehtoisia vakuutuksia, mutta tällöin uhrin on maksettava itse omavastuuosuus. Ansionmenetystä harvoin korvataan täysimääräisenä ja valtion oikeusapukin kattaa vain osan asianajokuluista, ja omavastuuosuus lasketaan uhrin tulojen mukaisesti.⁸³

Identiteettivarkauden uhrille yleisimmät taloudelliset seuraukset johtuvat siitä, mihin hänen identiteettiään on käytetty. Jos tekijä ottaa uhrin nimissä esimerkiksi lainaa, avaa puhelinliittymiä tai tilaa tuotteita verkosta, tästä aiheutuu uhrille taloudellisia kustannuksia. Tekijä saattaa myös käyttää uhrin tietoja vain saadakseen näitä sopimuksia tai tuotteita, mutta jättää ne tämän jälkeen maksamatta, jos hänellä ei kuitenkaan ole pääsyä uhrin tileille. Tällöin

⁸² Kjällman 2011, s. 38.

⁸³ Kjällman 2011, s. 38-39.

taas uhrille voi seurata maksuhäiriömerkintöjä tai hänet voidaan todeta luottokelvottomaksi, ja tapauksen selvittyäkin tästä voi jäädä uhrille merkintä luottohistoriaan, joka saattaa hankaloittaa uhrin taloudenhoitoa paljon myöhemminkin.⁸⁴ Tekijä voi myös päästä mahdollisten hakkeriohjelmien avulla käsiksi uhrin verkkopankkitunnuksiin, jolloin aiheutuva taloudellinen vahinko voi olla erityisen mittavaa. Jos tilitä on lähdössä erityisen suuria summia, pankki itse reagoi tapaukseen ja ottaa yhteyden tilin haltijaan. Tästä syystä tekijä usein siirtää tarpeeksi pieniä summia, etteivät pankin turvajärjestelmät reagoi siirtoihin. Tekijä saattaa esimerkiksi vaihtaa oman tilinsä jo lähtevään maksuun ja nostaa summaa vain pienesti, jolloin uhri ei osaa edes epäillä mitään rikollista toimintaa. Tilin haltija ei usein tajua joutuneensa rikoksen uhriksi ennen kuin hän saa muistutuksia maksamattomista laskuista tai tarkastaa tilinsä pääte-laitteelta jossa kyseistä hakkerointia ei ole, ja näkee tilinsä tyhjentyneen. On arvioitu, että pelkästään vuonna 2012 suomalaisilta tileiltä saatiin varastettua yhteensä lähes miljoona euroa, joista vain puolet onnistuttiin palauttamaan uhreille takaisin.⁸⁵

Vaikka identiteettivaras ei tavoittelisikaan taloudellista hyötyä vaan teon tarkoituksena on enemmänkin kiusanteko, saattaa uhrille aiheutua taloudellista haittaa. Jos uhrin nimissä julkaistaan esimerkiksi sosiaalisessa mediassa väärennettyä, vihamielistä, loukkaavaa tai uhkaavaa tietoa, voi uhri mahdollisesti menettää työnsä tai jonkin yksittäisen luottamuksellisen työtehtävänsä ja näiden seurauksena voi uhrille aiheutua kiusanteollisestakin identiteettivarkaudesta taloudellista haittaa ansionmenetyksen muodossa.⁸⁶ Identiteettivarkaudesta voi siis syntyä suoranaisesti taloudellista haittaa mikäli uhrin tilitä viedään rahaa tai hänen tiedoillaan ostetaan tuotteita tai palveluita, mutta taloudellista haittaa voi aiheutua myös pelkästään perintään menneiden maksamattomien laskujen johdosta. Lisäksi identiteettivarkautta voi seurata ansionmenetys, maksuhäiriömerkinnät tai luottokelpoisuuden menetys kokonaisuudessaan. Näiden jo tapahtuneiden taloudellisten menetysten lisäksi rikosprosessista itsestään voi aiheutua uhrille lisäkuluja, ja kaikista rikoksen seurauksena aiheutuneista kuluista uhri vain harvoin tulee saamaan takaisin menettämänsä summan kokonaisuudessaan, puhumattakaan aineettomista menetyksistä joita uhrille on aiheutunut.

3.2.3 Psyykkiset seuraukset

Kun henkilö joutuu rikoksen uhriksi, se vaikuttaa hänen elämäänsä usealla eri tasolla, ja osa seurauksista on huomattavissa välittömästi, osa vasta jonkin ajan kuluttua. Rikoksilla on paitsi selkeät seuraukset myös erilaisia välillisiä seurauksia. Vähimmillään rikoksen seuraukset ovat vain ohimenevä harmi ja katkeruus. Näin käy kuitenkin vain harvoissa tapauksissa, ja usein

⁸⁴ Tranberg & Heuer 2013, s. 95.

⁸⁵ Rousku 2014, s. 21.

⁸⁶ Rousku 2014, s. 16-17.

rikosta seuraa vähintäänkin pieni kriisi uhrin elämässä. Rikoksen vuoksi uhri voi kokea voimakasta ahdistusta ja epätietoisuutta, ja tästä huolimatta hänen on kyettävä huolehtimaan käytännön asioista annetuissa aikarajoissa sekä otettava selvää rikosprosessiin liittyvistä asioista. On todennäköistä ettei uhri tiedä laissa säädettyjä oikeuksiaan tai osaa kysyä oikeita kysymyksiä saadakseen tarvitsemaansa tietoa.⁸⁷ Uhri voi kokea tilanteen hallitsemattomana, sillä hän ei tiedä, mitä kaikkea varastetulla identiteetillä on ehditty tehdä tai voidaan vielä myöhemmin tehdä. Identiteettivarkauden selvitys ja vahinkojen minimalisointi on hidasta ja uuvuttavaa ja siitä aiheutuu uhrille sekä taloudellista että henkistä vahinkoa, joista uhri voi joutua kärsimään vuosia.⁸⁸

Rikoksen uhriksi joutuminen haastaa aina henkilön psyykkistä hyvinvointia ja aiheuttaa suoja-reaktioita, jotka vaikuttavat psyykkiseen toimintaan. Ensin uhri kokee sokkireaktion, jota seuraa varsinainen reaktiovaihe. Tämän jälkeen uhri pystyy työstämään ja käsittelemään tapahtunutta ja lopulta löytämään uuden suunnan itselleen. Sokki on automaattinen ensireaktio kun henkilö on kokenut jonkin järkyttävän tai äkillisen tapahtuman. Sokkireaktion voitaisiin sanoa olevan ihmisen kehon ja mielen tauko joka suojaa uhria liian voimakkailta tunteilta ja varmistaa, että uhri pysyy toimintakykyisenä. Sokkireaktion aikana uhri kokee usein tilanteen olevan epätodellinen, eikä hän pysty ajattelemaan selkeästi tai rationaalisesti. Sokki on yleensä lyhytaikainen ja välitön ensireaktio jolloin uhrista ei välttämättä edes huomaa, että hän todella reagoi tilanteeseen. Koska sokkireaktio on ensimmäinen vaihe rikoksen tapahduttua tai käytyä ilmi, ajoittuu rikosilmoituksen teko yleensä juuri kyseiseen vaiheeseen ja tällöin uhri ei välttämättä jälkeinpäin selkeästi muista, mitä neuvoja hän on viranomaisilta saanut.⁸⁹ Identiteettivarkautapauksissa uhri kokee sokkireaktion yleensä siinä vaiheessa kun rikos käy ilmi ja kun uhri saa tietoonsa toisen henkilön käyttäneen hänen henkilöllisyyttään rikollisiin tarkoituksiin. Tällöin uhrin on juuri sokkireaktionsa aikana pystyttävä toimimaan ja ajattelemaan nopeasti, jotta hänen on mahdollista tehdä kaikki suojaavat toimet ja aiheutuvat vahingot jäävät mahdollisesti pienemmiksi.

Kun uhri on päässyt sokkireaktion yli, alkavat todelliset tunteet nousta pintaan ja uhri alkaa pikku hiljaa ymmärtää mitä on tapahtunut ja mitä se kokonaisuudessaan tarkoittaa. Rikoksen uhriksi joutuminen voi aiheuttaa uhrissa uni- ja keskittymisvaikeuksia, ja tässä vaiheessa on uhrin kannalta tärkeintä, että tapaukselle ulkopuolinen henkilö auttaa uhria kokoamaan rikoksen faktat hänen kanssaan niin selkeäksi kokonaisuudeksi kuin mahdollista. Uhrin psyykkisen toipumisen kannalta on myös tärkeää, että hän palaa arkirutiineihinsa mahdollisimman pian tapahtuneen jälkeen. Omalta osaltaan myös rikoksen tutkinta ja sen eteneminen vaikut-

⁸⁷ Kjällman 2011, s. 21.

⁸⁸ Rikosuhripäivystys 2014. Viitattu 27.7.2017

⁸⁹ Kjällman 2011, s. 25-26.

tavat uhrin toipumisprosessiin. Jos rikostutkinta etenee nopeasti, voi se edesauttaa myös uhrin toipumista. Jos taas tutkinta ei tunnu etenevän, voi se vaikuttaa hidastavasti uhrin toipumiseen.⁹⁰ Jos siis esimerkiksi poliisi saa jäljitettyä identiteettivarkaan nopeasti tai pystyy ehkäisemään siitä aiheutuneita vaikutuksia, voi se edesauttaa uhrin toipumista, kun taas tapauksissa, joissa tekijää on vaikea tai mahdoton jäljittää ja suurta vahinkoa on jo ehtinyt tapahtua, saattaa uhrin toipuminen edetä hitaammin. Tällaisissa tapauksissa voi tekijä lisäksi jatkaa myöhemmin uhrin henkilötietojen käyttöä, joka taas osaltaan vaikuttaa uhriin ja mahdollisesti laukaisee uuden kriisin.

Kun uhri lopulta pystyy käsittelemään ja työstämään tapahtunutta, hän pystyy vihdoin prosessoimaan tapahtunutta ja siitä seuranneita menetyksiä. Tässä vaiheessa uhri saattaa vetäytyä ja vältellä tapahtuneesta puhumista, ja muistivaikeudet sekä keskittymisen vaikeus ovat yleensä tässä vaiheessa voimakkaimmillaan. Uhrin on myös valmistauduttava riittävän hyvin oikeudenkäyntiin, mikäli sellainen on tulossa, jotta tilanne ei ole uhrille jälleen uusi traumatisoiva kokemus. Yleisesti rikoksen seurauksena uhrin elämä tai sen osa-alueet muuttuvat, ja hänen on opittava hyväksymään rikostapahtumat ja sopeuduttava seuranneisiin muutoksiin. Kun uhri vihdoin pystyy yhdistämään rikoksesta aiheutuneen kokemuksen osaksi omaa historiaansa, voidaan hänen katsoa työstäneen onnistuneesti läpi kriisinsä. Tässä vaiheessa uhri pystyy ongelmitta puhumaan rikoksesta ja siitä aiheutuneista seurauksista sekä ottamaan vastaan uusia haasteita elämässään.⁹¹

Kun henkilö joutuu rikoksen uhriksi, hän saattaa käydä läpi useita eri tunnereaktioita. Yleisimpiä reaktioita ovat turvattomuuden tunne, pelko tai ahdistus, syyllisyys, häpeä sekä viha. Rikoksen uhri saattaa myös myöhemmässä vaiheessa kärsiä erilaisista ongelmista, kuten masennuksesta tai paniikkihäiriöstä. Rikosta seuraavat oireet eivät siis ole sidoksissa sairauksiin tai uhrin persoonaan, vaikka traumareaktiot aiheuttaisivatkin muutoksia uhrin sosiaalisiin suhteisiin, tunne-elämään, käyttäytymiseen tai persoonallisuuteen.⁹² Identiteettivarkauksissa uhri saattaa kokea menettäneensä identiteettinsä kokonaan, vaikei näin todellisuudessa ole. Reaktioihin vaikuttavat lisäksi teosta aiheutuvat seuraukset. Taloudellisten seurausten ohella identiteettivarkauden uhri saattaa kokea sosiaalisia seurauksia, jos hänen identiteetillään on esimerkiksi esiinnytty sosiaalisessa mediassa ja esitetty valheellista tietoa tai kerrottu arkaluontoisia asioita hänen yksityiselämästään. Sosiaaliset vaikutukset ja taloudelliset vaikutukset voivat myös linkittyä yhteen, jos uhri on identiteettivarkauden myötä esimerkiksi menettänyt mainettaan tai kunniaansa ja sen seurauksena menettänyt työpaikkansa ja työtoverinsa,

⁹⁰ Kjällman 2011, s. 26-27.

⁹¹ Kjällman 2011, s. 28-29.

⁹² Kjällman 2011, s. 30-36.

ja tieto on saattanut levitä myös alan muihin yrityksiin, jolloin tulevakin työnhaku saattaa hankaloitua huomattavasti.

3.3 Ennaltaehkäisy ja suojautuminen

Mistä tahansa rikoksesta puhuttaessa ennaltaehkäisy on aina merkittävässä ja tärkeässä roolissa. Ennaltaehkäisyä voidaan tarkastella eri näkökulmista, joita ovat tekijä-, uhri- ja tilanne- lähtöiset ennaltaehkäisyt. Ennaltaehkäisy voidaan jakaa kolmeen eri vaiheeseen, joista ensimmäinen kohdistuu laajalti yhteiskuntaan. Yhteiskunnan rooli rikosten ennaltaehkäisystä painottuu nimenomaisesti yleisen tason rikollisuuden ennaltaehkäisyyn, jonka kohderyhmään kuuluvat kaikki kansalaiset. Tärkeässä roolissa yleisessä rikosten ehkäisyssä on kansallinen rikoksantorjuntaohjelma, jonka avuksi on toteutettu sisäministeriön kokoamia sisäisen turvallisuuden ohjelmia. Sisäisen turvallisuuden ohjelmien yhteisenä tavoitteena on ollut yhteisten toimintapolitiikkojen luonti rikollisuuden vähentämiseksi ja turvallisuuden lisäämiseksi niin, että kaikessa julkisessa päätöksenteossa huomioidaan niiden vaikutukset rikollisuuteen.⁹³

Toissijaisesta ehkäisystä puhuttaessa painottuu ennaltaehkäisy rikollisuudesta johtuviin haitallisiin vaikutuksiin ja siihen, mitä näiden haittojen rajoittamisen tai vähentämisen eteen on mahdollista tehdä. Tällaisessa ennaltaehkäisyssä tulee huomioida uhrin ohella myös rikoksen todistajat ja uhrin lähipiiri sekä koko yhteisö, jossa rikos tapahtuu. Ehkäisytyö painottuu niiden viranomaisten ja kolmannen sektorin toimijoiden harteille, jotka kohtaavat uhreja auttaakseen ja tukeakseen heitä kokemuksen läpi. Tähän toissijaiseen ehkäisyyn voidaan laskea kuuluvaksi myös kaikki ne työt joita hallitusohjelman mukaan tehdään rikosuhrien aseman parantamisen vuoksi. Esimerkiksi Rikosuhripäivystys on hyvä esimerkki tällaisesta kolmannesta sektorista, joka toiminnallaan toteuttaa toissijaista ennaltaehkäisyä.⁹⁴

Kolmas ennaltaehkäisyvaihe taas tavoittelee rikosuhrien uudelleen uhriksi joutumisen mahdollisuuden rajoittamista. Tilastollisesti katsottuna voidaan todeta, että osa kansalaisista joutuu rikosten uhriksi toistuvasti, ja rikoksen uhriksi joutuminen jopa kasvattaa riskiä joutua uhriksi uudelleen. Kaikkien rikosuhrien kanssa tekemisissä olevien tahojen tulisi auttaa uhreja ratkaisujen tekemisessä jotka osaltaan edesauttaisivat välttämään uhriksi joutumista jatkossa. Jos uudelleen uhriksi joutumista ennaltaehkäistään onnistuneesti, vähentää se ratkaisevasti rikollisuutta kokonaisuutena, sillä suuressa osassa rikoksista uhreina on tietty pieni joukko kansalaisista. Kun henkilö joutuu toistuvasti rikoksen uhriksi, saattaa hän joutua huonon tai epäoikeudenmukaisen kohtelun alaiseksi ja tätä kautta joutuu rikoksen uhriksi järjestelmän kautta yhä uudelleen. Jotta kyseistä tapahtumaketjua voitaisiin välttää, tarvitaan rikoksen uhreja

⁹³ Kjällman 2011, s. 170.

⁹⁴ Kjällman 2011, s. 170-171.

kohtaaville tahoille jatkuvaa koulutusta ja kehittyviä toimintamalleja, ja suhtautumista uhreihin tulisi asiakaslähtöistä lisäämällä matalakynnyksisiä tukipalveluita.⁹⁵

Yhteiskunnalle painottuvan ennaltaehkäisyn lisäksi tärkeässä asemassa on aina kansalaisen itsensä toteuttama ennaltaehkäisy jokapäiväisessä elämässään sekä rikoksen jo tapahduttua uhrin omatoiminen suojautuminen rikoksen vaikutuksilta tai vähintäänkin vaikutusten minimoimiseksi. Identiteettivarkaudelta suojautuessa maalaisjärjen avulla on mahdollista päästä jo pitkälle.⁹⁶ Identiteetin suojaamisen merkitys on korostunut digiyhteiskunnan kasvun myötä ja melkein kuka vain voi joutua identiteettivarkauden uhriksi. Vaikka uhriksi joutuminen on aina mahdollista, ei se tarkoita etteikö ennaltaehkäisy tai suojautuminen olisi kannattavaa. Vaikka identiteettivarkaudelta suojautuminen ei olekaan kovin yksinkertaista, pääsee perusasioilla jo melko pitkälle ja jotain on kuitenkin aina tehtävissä.⁹⁷ Vaikka identiteettivarkaus ehtisikin jo tapahtua, on seurauksilta myös mahdollista suojautua tai vähintäänkin kontrolloida vahinkojen määrää. Näitä suojautumiskeinoja on listattu alla olevaan taulukkoon (taulukko 1), ja niitä avataan erikseen seuraavissa alakappaleissa.

<u>Suojautuminen verkossa</u>	<u>Suojautuminen arkielämässä</u>
<ul style="list-style-type: none"> • Virustorjuntaohjelmien ja muiden tietokonetta suojaavien ohjelmistojen päivitys ja ajantasaisuus • Riittävän vaikeat ja monimutkaiset salasanat • Kahdessa paikassa ei koskaan käytössä sama salasana • Kaikilla käyttäjätileillä käyttötarkoituksen mukaan säädetyt yksityisyysasetukset • Henkilötietoja annettaessa tulee harkita, onko sivusto luotettava ja millaiset yksityisyysasetukset sivustolla on • Google Alertsin hakulausekkeita seuraamalla saa nopeasti tietoonsa, jos tietojasi käytetään • Julkisia tai toisten henkilöiden tietokoneita 	<ul style="list-style-type: none"> • Paperipostin määrän vähentäminen • Laskujen tilaus e-laskuina verkkopankkiin • Lukollisen postilaatikon hankinta • Henkilötietoja sisältäviä papereita ei tulisi koskaan heittää lehtikeräykseen tai muihin paikkoihin, joista ne on helppo saada • Henkilötunnuksen suhteen tulisi olla erityisen varovainen, eikä sitä koskaan tule antaa tuntemattomille tai henkilöille, jotka eivät sitä tarvitse asiointiin • Salasanojen ja pin-koodien säilytys niin, etteivät ne voi vahingossakaan päätyä sivullisille • Maksukortin tunnuksen säilytys muualla kuin kortin yhteydessä tai läheisyydessä

⁹⁵ Kjällman 2011, s. 171.

⁹⁶ Haasio 2013, s. 47.

⁹⁷ Rikosuhripäivystys 2014. Viitattu 28.7.2017

<p>käytettäessä selaushistorian sekä loki- ja väliaikaistiedostojen tyhjennys</p> <ul style="list-style-type: none"> • Henkilökohtaisen tietokoneen selaimen välimuistin tyhjennys riittävän usein, ja esimerkiksi verkkopankkiasioinnin jälkeen tyhjennys heti • Verkkopankkimaksuissa käytössä on suojattu verkkoyhteys ja kauppaa tehdään luotettavan tahon kanssa • Kaksivaiheisen tunnistuksen käyttö • Pankkitunnuksia, salasanoja tai henkilötunnusta ei anneta sähköpostitse millekään taholle • Tuntemattomilta tahoilta tulleita sähköposteja tai niiden liitetiedostoja ei avata • Jos jokin verkossa vaikuttaa epäilyttävältä, varmuuden vuoksi ilmoitus viranomaisille • Huomion kiinnitys siihen, ketä sosiaalisessa mediassa hyväksyy kaverilistoilleen • Erilaisten linkkien klikkailun suhteen kannattaa myös noudattaa erityistä varovaisuutta • Erilaiset sovellukset voivat ottaa käyttöönsä mitä tahansa käyttäjätilitäsi löytyvää tietoa • Googlen kuvahausta omalla kuvallaan löytyvien osumien tarkastus • Ajan tasalla pysyminen uusimmista suojautumisohjeista 	<ul style="list-style-type: none"> • Tiliotteiden seuraus, jotta huomaa jos tilitä on lähdössä asiattomia maksuja • Väestörekisterikeskukseen, maistraattiin ja Trafiin on mahdollista tehdä tietojenluovutuskielto • Pankkikortin koodin peittäminen näppäillessä • Päiväkohtaisen nostorajan asettaminen käteistarpeen perusteella • Jos maksukorttiautomaatissa on havaittavissa jotakin outoa, tulee yhteys ottaa aina automaatin yhteydessä olevaan numeroon • Lompakon kadotessa kaikkien korttien sulkeminen välittömästi sekä ilmoitus poliisille varastetun lompakon sisällöstä
---	--

Taulukko 1: Identiteettivarkauksilta suojautuminen.

Vaikka identiteettivarkauksilta suojautumiselle ei ole täydellistä takuuta, saa ennaltaehkäisyllä ja varautumisella aikaan jo paljon. Yksinkertaisimmillaan voidaan ennaltaehkäisyä lähestyä siitä ajatuksesta, ettei henkilötietoja levitetä tarpeettomasti verkossa tai anneta ilman painavasti perusteltua syytä henkilötunnuksensa loppuosaa tai luottokortin numeroaan eteenpäin. Koska lähtökohtaisesti sosiaalisissa verkostoissa julkaistaan laajasti tietoa esimerkiksi syntymäaajoista, työpaikoista, sukulaisista ja osoitteista, tulisi henkilötunnuksen sisällyttämistä mihinkään asiakirjoihin tai sähköposteihin välttää. Kun henkilötunnus yhdistetään

muihin jaettuihin tietoihin, on luottokorttien hankinta ja muu taloudellisen vahingon aiheutus helppoa.⁹⁸ Vaikka henkilötietojen hakkerointi verkossa on myös mahdollista, ovat yleensä helpommin tavoitettavissa olevat tiedot identiteettivarkaille optimaalisempia eivätkä ne vaadi erityisiä tietoteknisiä taitoja. Myös perinteiset identiteettivarkaudet ovat edelleen suhteellisen yleisiä, joten henkilötietoja saatetaan etsiä myös laskuista, virallisista asiakirjoista tai esimerkiksi varastetun lompakon sisällöstä.⁹⁹

3.3.1 Verkkoidentiteettivarkauksien ennaltaehkäisy uhrin toimesta

Jos tarkastellaan verkossa ja sosiaalisessa mediassa tapahtuvien identiteettivarkauksien ennaltaehkäisyä, voidaan heti ensimmäisenä mainita virustorjuntaohjelmien ja muiden tietokoneita suojaavien ohjelmistojen päivitys ja ajantasaisuus. Itse tietokoneen sekä kaikkien käyttäjätilien ja sähköpostin salasanojen tulee olla riittävän vaikeita ja monimutkaisia, eikä kahdessa paikassa tulisi koskaan käyttää samaa salasanaa. Kaikilla käyttäjätileillä kannattaa myös tilin käyttötarkoituksesta riippuen säätää yksityisyysasetuksia, jolloin tietojen ulkopuolisille leviäminen rajoittuu ja vaikeutuu. Käyttäjätilien yksityisyysasetuksien kohdalla kannattaa kuitenkin huomioida, että palveluntarjoajat saattavat muuttaa asetuksiaan ilman erillisiä ennakkoilmoituksia, joten pelkästään yksityisyysasetusten avulla tiedot eivät ole selkeässä suojassa.¹⁰⁰ Aina henkilötietoja annettaessa tulee harkita onko kyseinen sivusto varmasti luotettava, ja millaiset yksityisyysasetukset sivustolla on.¹⁰¹ Google Alertsillä on myös mahdollista ottaa käyttöön erilaisia hakulausekkeita joita seuraamalla saa nopeasti tietoonsa, jos joku käyttää nimeäsi, puhelinnumeroasi, osoitetta tai muuta tietoasi.¹⁰²

Varsinkin julkisia tai toisten henkilöiden tietokoneita käytettäessä kannattaa muistaa selaushistorian sekä loki- ja väliaikaistiedostojen tyhjennys. Myös oman henkilökohtaisen tietokoneen selaimen välimuisti olisi hyvä tyhjentää melko usein, ja esimerkiksi verkkopankkiasioinnin jälkeen tyhjennys kannattaisi tehdä heti. Jos joku pääsee hakkeroimaan tietokoneen, on verkkohistorian kautta salasanojen ja käyttäjätunnusten selvittäminen helppoa kun selaushistoriaa ja välimuistia ei ole tyhjennetty.¹⁰³ Aina kun pankkikorttimaksuja tehdään verkossa, on varmistettava, että käytössä on suojattu verkkoyhteys ja kauppaa tehdään luotettavan tahon kanssa. Pankkitunnuksia, salasanoja tai henkilötunnusta ei koskaan tulisi antaa sähköpostitse millekään taholle eikä tuntemattomilta tahoilta tulleita sähköposteja tai niiden liitetiedostoja

⁹⁸ Vanto 2011, s. 69.

⁹⁹ Haasio 2013, s. 47.

¹⁰⁰ Forss 2014, s. 101.

¹⁰¹ Rikosuhripäivystys 2014. Viitattu 28.7.2017

¹⁰² Tranberg & Heuer 2013, s. 245.

¹⁰³ Haasio 2013, s. 123–125.

tulisi koskaan avata. Jos jokin verkossa vaikuttaa väärinkäytöltä, huijaukselta tai muuten epäilyttävältä, kannattaa siitä aina varmuuden vuoksi ilmoittaa viranomaisille.¹⁰⁴ Huomiota tulisi myös kiinnittää siihen, ketä sosiaalisessa mediassa hyväksyy kaverilistoilleen. Erilaisten linkkien klikkailun suhteen kannattaa myös noudattaa erityistä varovaisuutta siitäkin huolimatta, että joku lähipiiristäsi olisi kyseisen linkin jakanut. Linkki ei välttämättä todellisuudessa olekaan tuttavien itsensä jakama vaan kyseessä voi olla jonkinlainen haittaohjelma. Myös erilaisten sovellusten kohdalla tulee huomioida, että ne voivat ottaa käyttöönsä mitä tahansa käyttäjätietoa löytyvää tietoa. Hyvä tapa tarkastaa onko identiteetillä tehty esimerkiksi valeprofiileita, on tarkastaa Googlen kuvahausta omalla kuvallaan löytyvät osumat.¹⁰⁵ Verkossa tapahtuvat identiteettivarkaudet ja muut rikokset yleistyvät kasvavaa vauhtia ja keinoja syntyy jatkuvasti lisää. Myös erilaisia tarpeita ja paikkoja suojautumiselle syntyy jatkuvasti, ja aina olisikin hyvä pysyä ajan tasalla uusimmista suojautumisohjeista, jotta ennaltaehkäisy olisi mahdollisimman tehokasta.

3.3.2 Perinteisten identiteettivarkauksien ennaltaehkäisy uhrin toimesta

Perinteisiltä identiteettivarkauksilta suojautuminen on siinä määrin yksinkertaisempaa, etteivät rikosten tekotavat ole niin monikeinoisia kuin verkossa. Perinteisten identiteettivarkauksien ennaltaehkäisyyn on kuitenkin myös useita keinoja, kuten paperipostin määrän vähentäminen ja esimerkiksi laskujen tilaus e-laskuina verkkopankkiin tai lukollisen postilaatikon hankinta. Henkilötietoja sisältäviä papereita ei tulisi koskaan heittää lehtikeräykseen tai muihin paikkoihin joista ne on helppo saada. Henkilötunnuksen suhteen tulisi olla erityisen varovainen myös verkon ulkopuolella eikä sitä koskaan tule antaa tuntemattomille tai henkilöille, jotka eivät sitä tarvitse asiointiin. Esimerkiksi puhelinmyyjä ei tarvitse mihinkään henkilötunnusta, joten sitä ei tulisi tällöin hänelle koskaan antaa, eivätkä esimerkiksi pankkivirkailijat koskaan pyydä palvelun tunnistetietoja puhelimitse. Salasanojen ja pin-koodien säilytyksen pitäisi tapahtua niin, etteivät ne voi vahingossakaan päätyä sivullisille, eikä esimerkiksi maksukortin tunnusta tulisi ikinä säilyttää kortin yhteydessä tai läheisyydessä. Tiliotteita seurattaessa huomaa nopeasti jos tilitä on lähdössä asiattomia maksuja. Väestörekisterikeskukseen, maistraattiin ja Trafiin on myös mahdollista tehdä tietojenluovutuskielto, mutta se saattaa aiheuttaa arkielämään liittyviä haasteita kyseisten tahojen kanssa asioitaessa.¹⁰⁶

Pankkikortin skimmauksen tai muiden koodivarkaiden uhriksi joutumista voi ennaltaehkäistä peittämällä aina koodia näppäillessään toisella kädellä tai esimerkiksi lompakolla näppäilykäteensä, jolloin koodia on mahdotonta saada sivusta. Korteille voi myös asettaa päiväkohtaisen

¹⁰⁴ Haasio 2013, s. 134-135.

¹⁰⁵ Forss 2014, s. 101-102.

¹⁰⁶ Rikosuhripäivystys 2014. Viitattu 28.7.2017

nostorajan käteistarpeensa perusteella, jolloin kortilta ei voida varkauden yhteydessä nostaa kaikkia varoja ulos. Jos maksukorttiautomaatissa on havaittavissa jotakin outoa, tulee yhteys ottaa aina automaatin yhteydessä olevaan numeroon, jotta mahdolliset skimmauslaitteet huomataan mahdollisimman pian. Jos lompakko varastetaan, on tärkeää sulkea kaikki tarvittavat kortit välittömästi ja ilmoittaa poliisille varastetun lompakon sisällöstä, jolloin sitä on vähintäänkin vaikeampi väärinkäyttää.¹⁰⁷ Vaikka identiteettivarkauksien täydellinen ennaltaehkäisy on mahdotonta, pääsee maalaisjärjellä ja aiemmin mainituilla arkielämän ja verkkokäyttäytymisen huomioilla jo pitkälle. Paras suojautumiskeino on toki kaikkien näiden keinojen yhtäaikaista noudattaminen, mutta myös noudattamalla edes osaa niistä on identiteettivarkauden uhriksi joutuminen jo epätodennäköisempää.

3.3.3 Rikoksen vaikutusten minimalisointi ja vaikutuksilta suojautuminen

Kun henkilö on joutunut identiteettivarkauden uhriksi, on hänen suuremman taloudellisen vahingon välttämiseksi myös pystyttävä toimimaan mahdollisimman nopeasti kun selviää, että hänen identiteettiään on käytetty toisen henkilön toimesta. Mitä nopeammin identiteettivarkaus tulee uhrin tietoon, sitä todennäköisempää on, että hän pystyy välttämään taloudellisen vahingon syntymistä tai minimoimaan seurauksia. Perinteisten identiteettivarkauksien ollessa kyseessä on tärkeää, että esimerkiksi lompakon varastamisen jälkeen uhri sulkee mahdollisimman pian kaikki maksukortit ja ilmoittaa viranomaisille varastetuista tunnisteista kuten henkilökortista tai ajokortista. Myös pankkiin tulee aina ilmoittaa maksukortin varastamisesta tai katoamisesta.¹⁰⁸

Jos uhri saa tietoonsa, että hänen identiteettiään on käytetty omaisuuden hankkimiseen, sopimusten tekoon tai lainojen hakuun, on hänen myös mahdollista asettaa itselleen määrälläinen luottokielto vahinkojen minimoimiseksi. Jos taas identiteettivarkaus käy ilmi muulla tavoin, kannattaa uhrin varmistaa esimerkiksi väestörekisterikeskuksesta, että hänen osoitetietonsa ovat varmasti oikein. Jos näin ei ole, uhri voi korjata tiedot ja samalla ilmoittaa tietojensa väärinkäytöstä. Kun uhri tarkastaa mahdollisimman pian identiteettivarkauden selvittyä osoitetietonsa, pystyy hän mahdollisesti suojaamaan talouttaan tekijän verkkokauppatalouksilta tai muilta vastaavilta yrityksiltä ja mahdollisesti jo hankitut tai tilatut tuotteet on mahdollista peruuttaa tai selvittää sen tahon kanssa, josta ne ovat peräisin. Joka tapauksessa aina kun uhrin tietoja on käytetty omaisuuden hankkimiseen, tulee uhrin olla mahdollisimman pian yhteydessä myös niihin tahoihin, joilta kyseistä omaisuutta on ehditty tai yritetty hankkia.¹⁰⁹

¹⁰⁷ Poliisi. Maksukorttirikollisuus. Viitattu 28.7.2017

¹⁰⁸ Rikosuhripäivystys 2014. Viitattu 28.7.2017

¹⁰⁹ Rikosuhripäivystys 2014. Viitattu 28.7.2017

Kun taas tarkastelua painotetaan verkossa tapahtuviin identiteettivarkauksiin ja niiden seurauksilta suojautumiseen, voidaan heti alkuun mainita valeprofiilien ilmoittaminen ja niiden poistopyyntö palveluntarjoajan kautta. Aina kun joltain käyttäjätilitä, tietokoneelta tai sähköpostista on viety henkilötietoja, on tärkeää muistaa vaihtaa salasana paitsi kyseisestä palvelusta myös muista käytössä olevista palveluista. Salasanaa vaihdettaessa palautussähköpostiosoite tulee aina tarkistaa, jottei uusikin salasana päädy identiteettivarkaan hallinnoitavaksi. Tässä kohtaa korostuu myös se, että jos selaushistoria ja muut tunnistetiedot on asianmukaisesti tyhjennetty, on identiteettivarkas epätodennäköisemmin päässyt käsiksi useampaan palveluun uhrin tunnuksilla tai tiedoilla. Silloin kun uhrin käyttäjätillille on murtauduttu, tulee aina mahdollisuuksien mukaan tarkistaa kirjautumishistoria ja sulkea kaikki muut aktiiviset kirjautumiset. Jos identiteettivarkas on saanut haltuunsa uhrin verkkopankkitiedot tai kolmannen osapuolen maksupalvelun käyttäjätiedot on ensisijaisen tärkeää, että uhri sulkee verkkopankkitunnuksensa välittömästi ja ilmoittaa väärinkäytöstä pankille tai ilmoittaa palveluntarjoajalle väärinkäytöstä ja vaatii mahdollisten maksujen kumoamista tai maksupalvelutilin sulkemista, jos identiteettivarkas ei ole vielä ehtinyt palvelua käyttää. Parhaassa tapauksessa näin uhri välttää suurenkin taloudellisen menetyksen, tai jos rahaa on jo ehtinyt siirtyä tililtä, on se mahdollisesti helpompi jäljittää tai palauttaa.¹¹⁰

4 Johtopäätökset

Tässä opinnäytetyössä oli tarkoituksena selvittää identiteettivarkauden uhrin asemaa rikoksessa, hänen mahdollisuuksiaan ennaltaehkäistä ja suojautua identiteettivarkauksilta sekä tarkastella identiteettivarkauden seurauksena uhriin kohdistuvia vaikutuksia. Lisäksi tarkoituksena oli tarkastella identiteettivarkautta määritelmänä sekä selvittää lainuudistuksen taustoja ja verrata uudistusta ja sen tarvetta vanhaan lainsäädäntöön. Työn tarkoituksena oli antaa lukijalle kokonaiskuva siitä kuinka identiteettivarkaus määritellään, mitä siitä on säädetty, millaisia eri identiteettivarkauden tekotapoja ja motiiveja on ja kuinka identiteettivarkaus vaikuttaa uhriin sekä kuinka uhrin olisi mahdollista ennaltaehkäistä uhriksi joutumista tai suojautua rikoksen seurauksilta. Tarkoituksena työssä oli lähestyä aihetta pääasiassa uhrin näkökulmasta.

Tutkimuksessa on selvitetty, millaisia vaikutuksia identiteettivarkaudella on uhriin sekä kuinka identiteettivarkauksia on mahdollista ennaltaehkäistä tai rikoksen seurauksilta suojautua. Suojautumiskeinot on jaettu verkossa suojautumiseen ja arkielämässä suojautumiseen, ja näitä keinoja on tarkemmin kuvattu kappaleissa 3.3.1 ja 3.3.2 sekä listattu taulukossa 1. Tulosten perusteella voidaan todeta keinoja olevan useita, mutta keinot kuitenkin ovat melko yksinker-

¹¹⁰ Rikosuhripäivystys 2014. Viitattu 28.7.2017

taisia ja niitä on helppo soveltaa arkielämässä. Tuloksissa ilmenee myös muutamia ongelmia niin lainsäädännön kuin ennaltaehkäisyynkin osalta. Lainsäädännön osalta ongelmallisena voidaan nähdä sen vaatimukset tunnusmerkistön täyttymiselle sekä rikosten selvittämisen vaikeus ja toisaalta rikosten jatkuva yleistyminen. Esimerkiksi sisäministeriön henkilöllisyyden luomista koskevan hankkeen työryhmän mukaan identiteettivarkauden käsitteen tulisi kattaa myös teot, jotka loukkaavat henkilön itsemääräämisoikeutta aiheuttamatta selkeätä vahinkoa tai haittaa. Kuitenkin tunnusmerkistön täyttymiseksi uhrille tulisi aiheutua identiteettivarkauden seurauksena taloudellista vahinkoa tai vähäistä suurempaa haittaa, joka osaltaan rajoittaa identiteettivarkauksien selvittämistä ja pakottaa tietyissä tapauksissa viranomaiset turvautumaan aiemmin käytettyihin rikosnimikkeisiin, kuten kunnianloukkaukseen.

Kaikissa tapauksissa ei välttämättä edelleenkään täyty mikään varsinainen rikosnimike, jolloin uhri jää vieläkin yksin selvittämään rikosta. Ongelmallista kyseisten rikosten yleistymisessä on se, että viranomaiset kuormittuvat tapausten alle ja sen kautta valtaosa tapauksista tullaan syyttäjän toimesta mahdollisesti rajoittamaan vastaavalla tavalla kuin esimerkiksi kunnianloukkaus. Erityisesti tällainen rajaaminen tulisi todennäköisesti vaikuttamaan sosiaalisessa mediassa tapahtuviin identiteettivarkaukstopauksiin. Johtopäätöksenä voidaan nähdä, että vaikka lainuudistus on ollut merkittävä askel eteenpäin identiteettivarkauksien selvittämisen ja identiteettivarkaiden rankaisemisen kannalta, olisi siinä saattanut ollut tarve huomioida paremmin myös niitä rikoksia joista uhrille ei varsinaista taloudellista tai muuta suurempaa haittaa aiheudu. Lisäksi tulisi jo ennalta varautua siihen, että lisääntyvät ilmoitukset identiteettivarkauksista tulevat todennäköisesti kuormittamaan viranomaisia siinä määrin, että syyttäjän on rajattava tapauksia, ja tämän johdosta uhrille tulisi olla muita keinoja ja verkostoja tällaisten tapausten selvittämisen varalle.

Ennaltaehkäisyssä ongelmia voidaan nähdä taas siinä, että edelleen henkilötietoja sisältäviä asiakirjoja käsitellään yksityiselämässä huolimattomasti, arkaluontoisia henkilötietoja annetaan eteenpäin heikoin perustein ja tietokoneiden virusturvia ei pidetä ajan tasalla tai salaisuuksia riittävän tasokkaina ja vaikeina. Näistä ongelmista voidaan johtopäätöksenä nähdä, että kansalaiset eivät edelleenkään ole riittävän tietoisia siitä kuinka yleisiä rikoksia identiteettivarkaudet nykypäivänä ovat ja kuinka helposti identiteettivarkas voi saada tarvitsemiaan tietoja uhriltaan. Vaikka yleisiä turvallisuusohjeita niin verkkoon kuin muuhunkin yksityiselämään on suhteellisen helposti saatavilla, eivät harmillisen monet niitä noudata, vaikka suuri osa niistä on yleisessä tiedossa ja osa melkein pätevästä itsetänselvyyksiä. Jos identiteettivarkauksien yleisyys ja sen tekokeinot olisivat laajemmin tiedossa, olisi mitä todennäköisimmin huomattavasti useampi valmis suojaamaan henkilötietojaan ja tietokonettaan aktiivisemmin, mikä taas osaltaan hidastaisi huomattavasti kyseisten rikosten määrällistä kasvua.

Opinnäytetyön tärkeimpänä johtopäätöksenä voidaankin pitää sitä, että varsinkin uhrin omalla ennaltaehkäisyllä on suuri merkitys identiteettivarkauksien kasvun hidastamisessa ja pidemmällä tähtäimellä mahdollisesti jopa identiteettivarkauksien määrällisessä vähentämisessä. Myös identiteettivarkauden seurauksilta suojautumisen voidaan päätellä työn perusteella olevan tärkeässä roolissa paitsi taloudellisten ja sosiaalisten vaikutusten määrään, myös uhrin psyykkiseen hyvinvointiin ja rikoksesta toipumisen kestoon. Johtopäätökset perustuvat kirjoittajan tutkimaan aineistoon, lähdeartikkeleiden haastatteluihin ja viranomaistilastoihin, aiheesta ennestään tehtyihin tutkimustuloksiin ja rikoksen tekemuotoihin sekä aiheeseen perehtymisen pohjalta kirjoittajan itse tekemiin havaintoihin ja huomioihin. Opinnäytetyö osoitti, että vaikkei identiteettivarkauden uhriksi joutumista voi täysin estää, voi uhriksi joutumiseen vaikuttaa suurelta osin omalla toiminnallaan ja ennaltaehkäisyn kautta uhriksi joutumisen mahdollisuus laskee huomattavan pieneksi.

Tutkimuksen tulosten voidaan katsoa olevan hyödyllisiä, sillä niiden myötä lukijan on mahdollista ymmärtää identiteettivarkautta kokonaisuutena paremmin, ja tuloksissa on esitetty lukijalle keinoja ennaltaehkäistä omalla toiminnallaan identiteettivarkauden uhriksi joutumista. Lisäksi lukijalle tarjotaan keinoja myös jo tapahtuneesta identiteettivarkaudesta aiheutuvilta seurauksilta suojautumiselle. Lukijan on tämän opinnäytetyön avulla mahdollista ymmärtää paremmin niitä juridisia, sosiaalisia, taloudellisia ja psyykkisiä seurauksia, joita identiteettivarkauden uhri rikoksen jälkeen kokee sekä konkreettisemmin käsittää ennaltaehkäisyn ja suojautumisen merkitystä identiteettivarkauksissa.

Lähteet

Lakiluettelo

Henkilötietolaki 22.4.1999/523

Laki yksityisyyden suojasta työelämässä 13.8.2004/759

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621

Rikoslaki 19.12.1889/39

Suomen Perustuslaki 11.6.1999/731

Tietoyhteiskuntakaari 7.11.2014/917

Painetut lähteet

Biegelman, M. 2009. Identity Theft Handbook: Detection, Prevention, and Security. Hoboken, US: Wiley.

Castells, M. 2009. The Power of Identity: the Information Age: Economy, Society, and Culture Volume II. Malden: Wiley-Blackwell.

Forss, M. 2014. Fobban sosiaalisen median selviytymisopas. Helsinki: Crime time.

Haasio, A. 2013. Netin pimeä puoli. Helsinki: Suomalaisen kirjallisuuden seura.

Kjällman, P. 2011. Rikoksen uhrin käsikirja. Jyväskylä: PS-kustannus.

Korhonen, R. 2003. Perusrekisterit ja tietosuojat. Helsinki: Edita.

Korhonen, R. 2013. Identity Theft and the Finnish Identity Programme. In: KnowRiShT 2012. Knowledge Rights – Legal, Societal and Related Technological Aspects. 25 years of Data Protection in Finland, 285-292. Ed. Erich Schweighofer, Ahti Saarenpää, Janos Böszörményi. Vienna, Austria: OCG

Lång, J. & Tolvanen, H. 2016. Tietosuojalainsäädäntö. Helsinki: Talentum.

Pesonen, P. 2013. Sosiaalisen median lait. Helsinki: Helsingin kamari Oy

Rousku, R. 2014. Kyberturvaopas – Tietoturva kotona ja työpaikalla. Helsinki: Talentum.

Tranberg, P. & Heuer, S. 2013. Älä kerro kaikkea! Itsepuolustusopas verkkoon. Helsinki: Talentum.

Vanto, J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro Oy

Sähköiset lähteet

Eduskunta. Tietoverkkorikosdirektiivin täytäntöönpano. Viitattu 12.7.2017

https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/tietoverkkorikosdirektiivin-taytantonpano.aspx

Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU. Annettu 12 päivänä elokuuta 2013. Tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta. Viitattu 25.7.2017

<http://eur-lex.europa.eu/legal-content/fi/ALL/?uri=CELEX:32013L0040>

Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräksi siihen liittyviksi laeiksi. Viitattu 11.7.2017

<https://www.finlex.fi/fi/esitykset/he/2014/20140232#idp432926768>

Helsingin Sanomat, Satu Pajuriutta. Julkaistu: 25.2. 2:00 , Päivitetty: 25.2. 8:39, viitattu 19.7.2017

<http://www.hs.fi/kaupunki/art-2000005102683.html>

Norton, Marian Merritt. Identiteettivarkauden välttäminen. Viitattu 20.7.2017

<https://fi.norton.com/identity-theft-primer/article>

Oikeusministeriö. Tietojärjestelmiin kohdistuvia hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamista koskevan direktiivin 2013/40/EU kansallisia täytäntöönpanotoimia valmisteleva työryhmä (tietoverkkorikosdirektiivi-työryhmä). Työryhmän asettamispäätös. 27.9.2013. Viitattu 11.7.2017

http://www.hare.vn.fi/Uploads/19677/208684/ASETTAMISPAATOS_20131001021508_208684.pdf

OU Police department, the university of Oklahoma. Internet Safety. Viitattu 20.7.2017

<http://www.ou.edu/content/police/inetmenu/introduction.html>

Poliisi. Maksukorttirikollisuus. Viitattu 28.7.2017

<https://www.poliisi.fi/rikkokset/rikosilmioita/maksukorttirikollisuus>

Poliisi. Tietorikoksia. Viitattu 27.7.2017

<https://www.poliisi.fi/rikkokset/rikosilmioita/tietorikoksia>

Rikosuhripäivystys. Erilaisia rikoksia - Identiteettivarkaus. 2014. Viitattu 27.7.2017

<https://www.riku.fi/fi/erilaisia+rikoksia/identiteettivarkaus/>

Rikosuhripäivystys. Oppaat ja ohjeet - Identiteettivarkaus. 2014. Viitattu 27.7.2017

<https://www.riku.fi/fi/oppaat+ja+ohjeet/identiteettivarkaus/>

Sisäministeriö. Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. 15.12.2010. Viitattu 11.7.2017

https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79876/sm_322010.pdf?sequence=1

Viljanen, Vesa. Yksityisyyden suoja - Lainsäädäntö. 2013-2017. Viitattu 26.7.2017

<https://www.yksityisyydensuoja.fi/lains%C3%A4%C3%A4d%C3%A4nt%C3%B6>

Taulukot

Taulukko 1: Identiteettivarkauksilta suojautuminen.	31
--	----

